aws

Entwicklerhandbuch

Amazon Route 53

API-Version 2013-04-01

Amazon Route 53: Entwicklerhandbuch

Table of Contents

Was ist Amazon Route 53?

Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS)-Web-Service. Sie können Route 53 zum Durchführen von drei wesentlichen Aufgaben in beliebiger Kombination verwenden: Domänenregistrierung, DNS-Routing und Zustandsprüfung.

Wenn Sie Route 53 für alle drei Funktionen verwenden möchten, beachten Sie bitte die nachstehende Reihenfolge:

1. Registrieren von Domänennamen

   Ihre Website benötigt einen Namen, zum Beispiel example.com. Mit Route 53 können Sie einen Namen für Ihre Website oder Webanwendung registrieren, bekannt als Domänenname.

   - Eine Übersicht finden Sie unter Funktionsweise der Domainregistrierung.
   - Ein entsprechendes Verfahren ist unter Registrieren einer neuen Domain beschrieben.
   - Ein Tutorial zum Registrieren einer Domäne und zum Erstellen einer einfachen Website in einem Amazon-S3-Bucket finden Sie unter Erste Schritte mit Amazon Route 53.

2. Weiterleiten des Internetdatenverkehrs an die Ressourcen für Ihre Domäne

   Wenn ein Benutzer einen Webbrowser öffnet und Ihren Domänennamen (example.com) oder Subdomänennamen (z. B. acme.example.com) in die Adressleiste ein, hilft Route 53 dabei, den Browser mit Ihrer Website oder Webanwendung zu verbinden.

   - Eine Übersicht finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird.
   - Die entsprechenden Verfahren sind unter Konfigurieren von Amazon Route 53 als DNS-Service beschrieben.
   - Eine Anleitung zum Weiterleiten von E-Mails an Amazon WorkMail finden Sie unterWeiterleitung des Datenverkehrs an Amazon WorkMail.

3. Überprüfen des Zustands Ihrer Ressourcen

   Route 53 sendet automatisierte Anfragen über das Internet zu einer Ressource, beispielsweise einem Webserver, um zu überprüfen, ob sie erreichbar, verfügbar und funktionsfähig ist. Sie können sich auch benachrichtigen lassen, wenn eine Ressource nicht mehr verfügbar ist, und den Internetdatenverkehr weg von fehlerhaften Ressourcen leiten.

   - Eine Übersicht finden Sie unter So überprüft Amazon Route 53 den Zustand Ihrer Ressourcen.

- Die entsprechenden Verfahren sind unter Amazon Route 53-Zustandsprüfungen erstellen beschrieben.

Weitere Funktionen von Route 53

Route 53 ist nicht nur ein DNS-Webdienst (Domain Name System), sondern bietet auch die folgenden Funktionen:

VPC-Resolver

Holen Sie sich rekursives DNS für Ihr Amazon VPCs VPCs in AWS-Regionen, in AWS Outposts Racks oder anderen lokalen Netzwerken. Erstellen Sie bedingte Weiterleitungsregeln und Route 53-Endpunkte, um benutzerdefinierte Namen aufzulösen, die in privat gehosteten Route 53-Zonen oder auf Ihren lokalen DNS-Servern verwaltet werden.

Weitere Informationen finden Sie unter. Was ist Route 53 VPC Resolver?

Amazon Route 53 Resolver auf Outposts

Connect VPC Resolver auf Outpost-Racks über Resolver-Endpunkte mit DNS-Servern in Ihren lokalen Rechenzentren. Dies ermöglicht die Auflösung von DNS-Abfragen zwischen den Outposts-Racks und Ihren anderen lokalen Ressourcen.

Weitere Informationen finden Sie unter. Was ist Amazon Route 53 auf Outposts?

Resolver-DNS-Firewall

Schützen Sie Ihre rekursiven DNS-Abfragen im VPC Resolver. Erstellen Sie Domainlisten und erstellen Sie Firewallregeln, die ausgehenden DNS-Verkehr anhand dieser Regeln filtern.

Weitere Informationen finden Sie unterVerwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr.

Verkehrsfluss

Easy-to-use und kostengünstiges globales Verkehrsmanagement: Leiten Sie Endbenutzer auf der Grundlage von Geonähe, Latenz, Integrität und anderen Überlegungen zum besten Endpunkt für Ihre Anwendung weiter.

Weitere Informationen finden Sie unterVerwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr.

Amazon-Route-53-Profile

Mit Route 53 53-Profilen können Sie DNS-bezogene Route 53-Konfigurationen auf viele VPCs und unterschiedliche Arten anwenden und verwalten. AWS-Konto

Weitere Informationen finden Sie unter. Was sind Amazon Route 53 53-Profile?

Themen

Funktionsweise der Domainregistrierung

Wenn Sie eine Website oder eine Webanwendung erstellen möchten, müssen Sie zunächst den Namen Ihrer Website registrieren. Dies wird auch als domain name bezeichnet. Ihr Domänenname ist der Name, z. B. example.com, den Ihre Benutzer in einen Browser eingeben, um Ihre Website anzuzeigen.

Im Folgenden finden Sie eine Übersicht darüber, wie Sie einen Domainnamen bei Amazon Route 53 registrieren:

1. Wählen Sie einen Domänennamen aus und vergewissern Sie sich, dass dieser verfügbar ist. Das bedeutet, dass niemand anders den Domänennamen registriert hat.

   Wenn der gewünschte Domänenname bereits verwendet wird, können Sie einen anderen Namen versuchen oder nur die Top-Level-Domain wie .com in eine andere Top-Level-Domain wie z. B. .ninja oder .hockey ändern. Eine Liste der Top-Level-Domains (Domänen oberster Ebene), die Route 53 unterstützt, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

2. Sie registrieren den Domänennamen mit Route 53. Wenn Sie eine Domäne registrieren, geben Sie Namen Kontaktinformationen für den Domäneneigentümer und andere Kontakte an.

   Wenn Sie eine Domäne mit Route 53 registrieren, wird der Service automatisch der DNS-Service für die Domäne und führt Folgendes aus:

   - Erstellt eine hosted zone, die denselben Namen hat wie die Domäne.
   - Weist eine Gruppe von vier Namenservern zur gehosteten Zone zu. Wenn jemand einen Browser für den Zugriff auf Ihre Website verwendet, wie z. B. www.example.com, teilt dieser Namenserver dem Browser den Speicherort Ihrer Ressourcen mit, wie z. B. ein Webserver oder ein Amazon-S3-Bucket. (Amazon S3 ist der Objektspeicher zum Speichern und Abrufen beliebiger Datenmengen von überall im Internet. Ein Bucket ist ein Container für Objekte, die Sie in S3 speichern.)
   - Ruft die Namenserver aus der gehosteten Zone ab und fügt sie zur Domäne hinzu.

   Weitere Informationen finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird.
3. Nach dem Registrierungsprozess senden wir Ihre Informationen an die Vergabestelle für die Domäne. Die domain registrar ist entweder Amazon Registrar, Inc. oder unsere Partner-Vergabestelle, Gandi. Die zuständige Vergabestelle für Ihre Domäne finden Sie unter Wie Sie Ihre Vergabestelle finden.
4. Die Vergabestelle sendet Ihre Informationen zur Registrierungsstelle für die Domäne. Eine Registrierungsstelle ist ein Unternehmen, das Domänenregistrierungen für eine oder mehrere Domänen oberster Ebene (Top-Level-Domänen), wie z. B. .com, verkauft.
5. Die Registrierungsstelle speichert die Informationen über Ihre Domäne in ihrer eigenen Datenbank und speichert auch einige Informationen in der öffentlichen WHOIS-Datenbank.

Weitere Informationen zum Registrieren eines Domänennamens finden Sie unter Registrieren einer neuen Domain.

Wenn Sie bereits einen Domänennamen bei einer anderen Vergabestelle registriert haben, können Sie die Domänenregistrierung an Route 53 übertragen. Dies ist nicht erforderlich, um andere Route-53-Funktionen zu nutzen. Weitere Informationen finden Sie unter Übertragen der Registrierung für eine Domain an Amazon Route 53.

Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird

Alle Computer im Internet, von Ihrem Smartphone oder Laptop aus, stellen eine Verbindung zu den Servern her, die Inhalte für riesige Einzelhandels-Websites bereitstellen, und kommunizieren über Nummern miteinander. Diese Zahlen, bekannt als IP-Adressen, liegen in einem der folgenden Formate vor:

- Format des Internetprotokolls, Version 4 (IPv4), z. B. 192.0.2.44
- Internetprotokollformat, Version 6 (IPv6), z. B. 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345

Wenn Sie einen Browser öffnen und eine Website aufrufen, müssen Sie sich nicht eine lange Zeichenfolge merken und eingeben. Stattdessen können Sie einen Domainnamen wie example.com eingeben und trotzdem an der richtigen Stelle ankommen. Ein DNS-Service wie Amazon Route 53 hilft dabei, die Verbindung zwischen Domainnamen und IP-Adressen herzustellen.

Themen

Übersicht über das Konfigurieren von Amazon Route 53, um Internetdatenverkehr an Ihre Domain weiterzuleiten

Im Folgenden finden Sie eine Übersicht über die Verwendung der Amazon-Route-53-Konsole zur Registrierung eines Domainnamens und zur Konfiguration von Route 53, um Internetdatenverkehr an Ihre Website oder Webanwendung weiterzuleiten.

1. Registrieren Sie den Domänennamen, den Ihre Benutzer für den Zugriff auf Ihre Inhalte verwenden sollen. Eine Übersicht finden Sie unter Funktionsweise der Domainregistrierung.
2. Nachdem Sie Ihren Domänennamen registriert haben, erstellt Route 53 automatisch eine öffentliche gehostete Zone, die denselben Namen wie die Domäne trägt. Weitere Informationen finden Sie unter Arbeiten mit öffentlichen gehosteten Zonen.
3. Um den Datenverkehr an Ihre Ressourcen weiterzuleiten, erstellen Sie Datensätze, auch als Ressourcendatensätze bezeichnet, in Ihrer gehosteten Zone. Jeder Datensatz enthält

Informationen darüber, wie Sie den Datenverkehr für Ihre Domain weiterleiten möchten, z. B. die folgenden:

Name

Der Name des Datensatzes entspricht dem Domänennamen (example.com) oder Unterdomänennamen (www.example.com, retail.example.com), für den Route 53 den Datenverkehr weiterleiten soll.

Der Name jedes Datensatzes in einer gehosteten Zone muss mit dem Namen der gehosteten Zone enden. Wenn der Name der gehosteten Zone beispielsweise auf example.com endet, müssen alle Datensatznamen auf example.com enden. Die Route-53-Konsole übernimmt dies automatisch für Sie.

Typ

Der Datensatztyp bestimmt in der Regel den Typ der Ressource, an die der Datenverkehr weitergeleitet werden soll. Wenn Sie beispielsweise den Datenverkehr an einen E-Mail-Server weiterleiten möchten, geben Sie MX als Typ ein. Um den Datenverkehr an einen Webserver weiterzuleiten, der über eine IP-Adresse verfügt, geben Sie A als Typ an. IPv4

Wert

Der Wert ist eng mit dem Typ verbunden. Wenn Sie MX als Typ angeben, geben Sie den Namen eines oder mehrerer E-Mail-Server als Wert ein. Wenn Sie A für Typ angeben, geben Sie eine IP-Adresse im IPv4 Format an, z. B. 192.0.2.136.

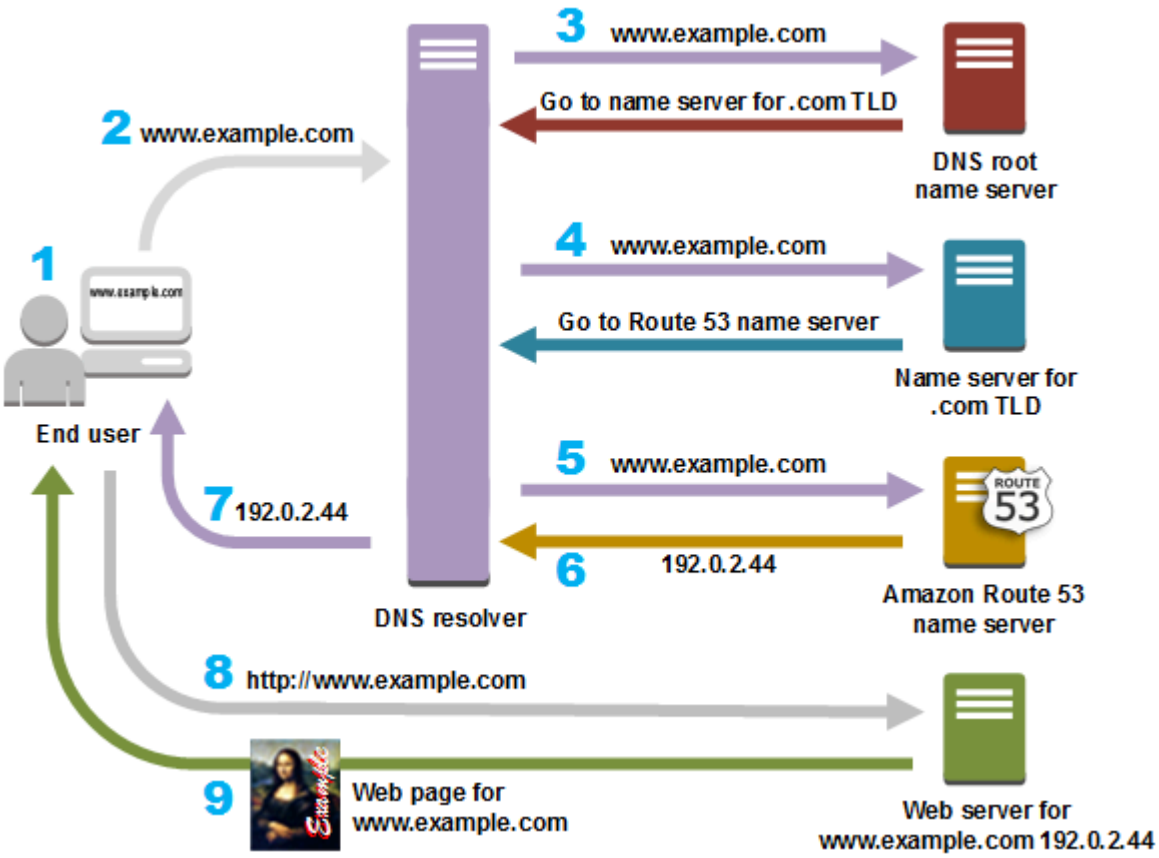
Weitere Informationen über Einträge finden Sie unter Arbeiten mit Datensätzen.

Sie können auch spezielle Route 53-Datensätze, sogenannte Alias-Datensätze, erstellen, die den Datenverkehr an Amazon S3 S3-Buckets, CloudFront Amazon-Distributionen und andere AWS Ressourcen weiterleiten. Weitere Informationen erhalten Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen und Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Ausführlichere Informationen über das Weiterleiten von Internetdatenverkehr an Ihre Ressourcen finden Sie unter Konfigurieren von Amazon Route 53 als DNS-Service.

So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter

Nach der Konfiguration von Amazon Route 53 zur Weiterleitung des Internetdatenverkehrs an Ihre Ressourcen, wie z. B. Webserver oder Amazon-S3-Buckets, geschieht innerhalb weniger Millisekunden Folgendes, wenn ein Benutzer Inhalte www.example.com anfordert:



1. Ein Benutzer öffnet einen Webbrowser, gibt www.example.com in die Adresszeile ein und drückt die Eingabetaste.
2. Die Anforderung für www.example.com wird an einen DNS-Auflöser weitergeleitet, die in der Regel vom Internetdienstanbieter (ISP) des Benutzers verwaltet wird, z. B. ein Kabelanbieter, ein DSL-Breitbandanbieter oder ein Unternehmensnetzwerk.
3. Der DNS-Auflöser des ISP leitet die Anforderung für www.example.com an einen DNS-Stamm-Namenserver weiter.
4. Der DNS-Resolver leitet die Anforderung von www.example.com erneut weiter, diesmal an einen der TLD-Namenserver für .com-Domänen. Der Namenserver für .com-Domänen beantwortet die Anforderung mit den Namen der vier Route-53-Namenserver, die der Domäne example.com zugeordnet sind.

Der DNS-Resolver speichert die vier Route-53-Namenserver im Cache. Wenn ein Benutzer das nächste Mal example.com aufruft, überspringt der Resolver die Schritte 3 und 4, weil die Namenserver für example.com bereits ermittelt wurden. Die Namenserver werden in der Regel für zwei Tage im Zwischenspeicher gehalten.

5. Der DNS-Resolver wählt einen Route-53-Namenserver aus und leitet die Anforderung von www.example.com an diesen Namenserver weiter.
6. Der Route-53-Namenserver sucht in der gehosteten Zone von example.com nach dem Datensatz für www.example.com, ruft den zugehörigen Wert ab (z. B. die IP-Adresse für einen Webserver, 192.0.2.44) und gibt die IP-Adresse an den DNS-Auflöser zurück.
7. Der DNS-Resolver verfügt schließlich über die IP-Adresse, die der Benutzer benötigt. Der Auflöser gibt den Wert an den Webbrowser zurück.

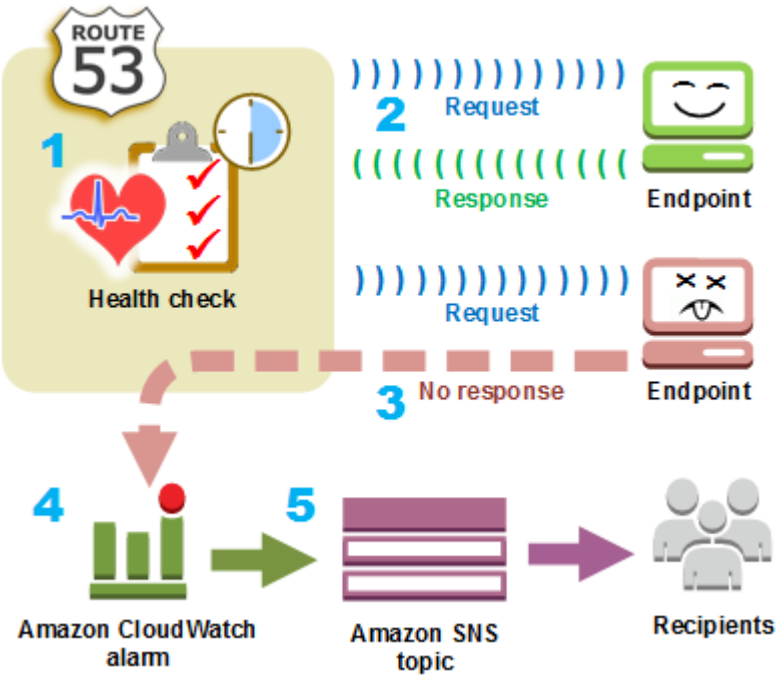
> **Note**
>
> Der DNS-Resolver behält außerdem die IP-Adresse für example.com für eine von Ihnen festgelegte Dauer im Zwischenspeicher, damit er schneller reagieren kann, wenn erneut ein Benutzer example.com aufruft. Weitere Informationen finden Sie unter time to live (TTL).

8. Der Webbrowser sendet eine Anforderung für www.example.com an die IP-Adresse, die er vom DNS-Resolver erhalten hat. Hier handelt es sich bei Ihren Inhalten beispielsweise um einen Webserver, der auf einer EC2 Amazon-Instance läuft, oder um einen Amazon S3-Bucket, der als Website-Endpunkt konfiguriert ist.
9. Der Webserver bzw. die jeweilige Ressource unter 192.0.2.44 gibt die Webseite für www.example.com an den Webbrowser zurück, und der Webbrowser zeigt die Seite an.

So überprüft Amazon Route 53 den Zustand Ihrer Ressourcen

Amazon-Route-53-Zustandsprüfungen überwachen den Zustand Ihrer Ressourcen, wie z. B. Webserver und E-Mail-Server. Sie können optional CloudWatch Amazon-Alarme für Ihre Gesundheitschecks konfigurieren, sodass Sie eine Benachrichtigung erhalten, wenn eine Ressource nicht verfügbar ist.

Im Folgenden finden Sie einen Überblick darüber, wie die Zustandsprüfung funktioniert, wenn Sie benachrichtigt werden möchten, wenn eine Ressource nicht mehr verfügbar ist:



1. Sie erstellen eine Zustandsprüfung und geben die Werte an, die bestimmen, wie die Zustandsprüfung funktionieren soll, zum Beispiel:
   - IP-Adresse oder Domänenname des Endpunkts, z. B. eines Webservers, den Route 53 Sie überwachen soll. (Sie können auch den Status anderer Zustandsprüfungen oder den Status eines CloudWatch Alarms überwachen.)
   - Das Protokoll, das Amazon Route 53 ausführen solle, um die Überprüfung durchzuführen: HTTP, HTTPS oder TCP.
   - Wie häufig Route 53 eine Anforderung an den Endpunkt senden soll. Das ist das Anforderungsintervall.
   - Wie viele aufeinanderfolgende Male der Endpunkt Anforderungen nicht beantwortet, bevor Route 53 ihn als nicht betriebsbereit betrachtet. Das ist der Fehlerschwellenwert.
   - Optional legen Sie fest, wie Sie benachrichtigt werden möchten, wenn Route 53 erkennt, dass der Endpunkt fehlerhaft ist. Wenn Sie die Benachrichtigung konfigurieren, setzt Route 53 automatisch einen CloudWatch Alarm. CloudWatch verwendet Amazon SNS, um Benutzer darüber zu informieren, dass ein Endpunkt fehlerhaft ist.
2. Route 53 beginnt, in den von Ihnen in der Zustandsprüfung angegebenen Intervallen Anforderungen an den Endpunkt zu senden.

   Wenn der Endpunkt auf die Anforderungen antwortet, betrachtet Route 53 den Endpunkt als fehlerfrei und führt keine Aktion aus.

3. Wenn der Endpunkt nicht reagiert, beginnt Route 53, die Anzahl aufeinander folgender Anforderungen, auf die der Endpunkt nicht reagiert hat, zu zählen:
   - Wenn die Anzahl den angegebenen Fehlerschwellenwert erreicht, betrachtet Route 53 den Endpunkt als fehlerhaft (nicht betriebsbereit).
   - Wenn der Endpunkt erneut reagiert, bevor die Anzahl den Ausfallschwellenwert erreicht, setzt Route 53 die Anzahl auf 0 zurück und kontaktiert Sie CloudWatch nicht.
4. Wenn Route 53 den Endpunkt für fehlerhaft hält und Sie die Benachrichtigung für die Zustandsprüfung konfiguriert haben, benachrichtigt Route 53. CloudWatch

   Wenn Sie keine Benachrichtigung konfiguriert haben, können Sie den Status Ihrer Route-53-Zustandsprüfungen in der Route-53-Konsole sehen. Weitere Informationen finden Sie unter Den Status von Zustandsprüfungen überwachen und Benachrichtigungen erhalten.
5. Wenn Sie die Benachrichtigung für die Zustandsprüfung konfiguriert haben, CloudWatch wird ein Alarm ausgelöst und Amazon SNS verwendet, um Benachrichtigungen an die angegebenen Empfänger zu senden.

Zusätzlich zur Prüfung der Integrität eines bestimmten Endpunkts können Sie eine Zustandsprüfung konfigurieren, um den Status eines oder mehrerer anderer Zustandsprüfungen zu überwachen, damit Sie benachrichtigt werden, wenn eine bestimmte Anzahl von Ressourcen, wie zum Beispiel zwei Webserver von fünf, nicht zur Verfügung stehen. Sie können auch eine Integritätsprüfung konfigurieren, um den Status eines CloudWatch Alarms zu überprüfen, sodass Sie anhand einer Vielzahl von Kriterien benachrichtigt werden können, nicht nur, ob eine Ressource auf Anfragen reagiert.

Wenn Sie über mehrere Ressourcen verfügen, die dieselbe Funktion ausführen, z. B. Webserver oder Datenbankserver, und Sie möchten, dass Route 53 den Datenverkehr nur an die fehlerfreien Ressourcen leitet, können Sie DNS-Failover konfigurieren, indem Sie eine Zustandsprüfung mit jedem Datensatz für diese Ressource verknüpfen. Wenn eine Zustandsprüfung feststellt, dass die zugrunde liegende Ressource fehlerhaft ist, leitet Route 53 den Datenverkehr weg von dem entsprechenden Datensatz.

Weitere Informationen über die Verwendung von Route 53 zur Überwachung des Zustand Ihrer Ressourcen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

Amazon-Route-53-Konzepte

Im Folgenden finden Sie eine Übersicht über die Konzepte, die in Amazon-Route-53-Entwicklerhandbuch erläutert werden.

Themen

Konzepte zur Domänenregistrierung

Im Folgenden finden Sie eine Übersicht über die Konzepte im Zusammenhang mit der Domänenregistrierung.

- domain name
- domain registrar
- domain registry
- domain reseller
- top-level domain (TLD)

Domänenname

Der Name (z. B. example.com), den ein Benutzer in die Adresszeile eines Webbrowsers für den Zugriff auf eine Website oder eine Webanwendung eingibt. Um Ihre Website oder Webanwendung im Internet verfügbar zu machen, registrieren Sie zunächst einen Domänennamen. Weitere Informationen finden Sie unter Funktionsweise der Domainregistrierung.

Domänenvergabestelle

Ein Unternehmen, das von der ICANN (Internet Corporation for Assigned Names and Numbers) für die Bearbeitung von Domainregistrierungen für bestimmte Top-Level-Domains (TLDs) akkreditiert ist. Die Vergabestelle für Ihre Domäne finden Sie unter Wie Sie Ihre Vergabestelle finden.

Domänenregistrierungsstelle

Ein Unternehmen, welches das Recht besitzt, Domänen mit einer bestimmten Domäne oberster Ebene (Top-Level-Domain, TLD) zu verkaufen. VeriSignIst zum Beispiel die Registry, die das Recht besitzt, Domains mit der TLD .com zu verkaufen. Eine Domänenregistrierungsstelle definiert die Regeln für die Registrierung einer Domäne, wie z. B. Residenzanforderungen für eine geografische TLD. Eine Domänenregistrierungsstelle verwaltet außerdem die autoritative Datenbank für alle Domänennamen mit derselben TLD. Die Datenbank der Registrierungsstelle enthält Informationen wie z. B. Kontaktinformationen und die Namenserver für die einzelnen Domänen.

Domänen-Reseller

Ein Unternehmen, das Domänennamen für Vergabestellen wie Amazon Registrar verkauft. Amazon Route 53 ist ein Domain-Reseller für Amazon Registrar und für unsere Partner-Vergabestelle, Gandi.

Top-Level-Domain (TLD)

Der letzte Teil eines Domänennamens, z. B. .com, .org oder .ninja. Es gibt zwei Typen von Top-Level-Domains:

Generische Top-Level-Domains

Diese geben Benutzern in der TLDs Regel eine Vorstellung davon, was sie auf der Website finden werden. Beispiel: Domänennamen mit der TLD .bike gehören oft zu Websites für Unternehmen oder Organisationen im Zusammenhang mit Motorrädern oder Fahrrädern. Mit wenigen Ausnahmen können Sie jede beliebige generische TLD verwenden, sodass ein Fahrradclub auch .hockey als TLD für ihren Domänenamen verwenden könnte.

Geografische Top-Level-Domains

Diese TLDs sind mit geografischen Gebieten wie Ländern oder Städten verknüpft. Einige Register für geografische Gebiete TLDs haben Wohnsitzerfordernisse, während andere beispielsweise die Verwendung als the section called “.io (Britisches Territorium im Indischen Ozean)” generische TLD zulassen oder sogar fördern.

Eine Liste der Optionen TLDs , die Sie bei der Registrierung eines Domainnamens bei Route 53 verwenden können, finden Sie unter. Domains, die Sie mit Amazon Route 53 registrieren können

Domain Name System(DNS)-Konzepte

Im Folgenden finden Sie eine Übersicht über die Konzepte im Zusammenhang mit dem Domain Name System (DNS).

- alias record
- authoritative name server
- CIDR block
- DNS query
- DNS resolver
- Domain Name System (DNS)
- hosted zone
- IP address
- name servers
- private DNS
- recursive name server
- record (DNS record)
- reusable delegation set
- routing policy
- subdomain
- time to live (TTL)

Alias-Datensatz

Ein Datensatztyp, den Sie mit Amazon Route 53 erstellen können, um den Datenverkehr an AWS Ressourcen wie CloudFront Amazon-Distributionen und Amazon S3-Buckets weiterzuleiten. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Autoritativer Namenserver

Ein Namenserver mit definitiven Informationen über einen Teil des Domain Name System (DNS), der Anforderungen von einem DNS-Auflöser beantwortet, indem er die entsprechenden Informationen zurückgibt. Beispielsweise kennt ein autoritativer Namenserver für die Top-Level-

Domain (TLD) .com die Namen der Namenserver für jede registrierte .com-Domäne. Wenn ein autoritativer .com-Namenserver eine Anforderung von einem DNS-Auflöser für example.com erhält, antwortet er mit den Namen der Namenserver für den DNS-Service für die Domäne example.com.

Route-53-Namenserver sind die autoritativen Namenserver für jede Domäne, die Route 53 als DNS-Service verwendet. Die Nameserver wissen basierend auf den Datensätzen, die Sie in der gehosteten Zone für die Domäne erstellt haben, wie Sie den Datenverkehr für Ihre Domäne und Subdomänen weiterleiten möchten. (Route-53-Namenserver speichern die gehosteten Zonen für die Domänen, die Route 53 als DNS-Service verwenden.)

Wenn beispielsweise ein Route-53-Namenserver eine Anforderung für www.example.com empfängt, sucht er diesen Datensatz und gibt die IP-Adresse zurück, z. B. 192.0.2.33, die im Datensatz angegeben ist.

CIDR-Block

Ein CIDR-Block ist ein IP-Bereich, der mit IP-basiertem Routing verwendet wird. In Route 53 können Sie den CIDR-Block von /0 bis /24 für und/0 bis /48 für IPv4 angeben. IPv6 Ein IPv4 /24-CIDR-Block umfasst beispielsweise 256 zusammenhängende IP-Adressen. Sie können Sätze von CIDR-Blöcken (oder IP-Bereichen) in CIDR-Standorten gruppieren, die wiederum in wiederverwendbaren CIDR-Sammlungen gruppiert sind.

DNS-Abfrage

Normalerweise eine Anforderung, die von einem Gerät, z. B. einem Computer oder Smartphone, für eine Ressource, die einem Domänennamen zugeordnet ist, an das Domain Name System (DNS) gesendet wird. Der häufigste Beispiel für eine DNS-Abfrage ist, wenn ein Benutzer einen Browser öffnet und den Domänennamen in die Adresszeile eingibt. Die Antwort auf eine DNS-Abfrage ist in der Regel die IP-Adresse, die einer Ressource zugeordnet ist, wie zum Beispiel einem Webserver. Das Gerät, das die Anforderung initiiert hat, verwendet die IP-Adresse für die Kommunikation mit der Ressource. Beispielsweise kann ein Browser die IP-Adresse verwenden, um eine Webseite von einem Webserver abzurufen.

DNS-Auflöser

Ein DNS-Server, der häufig von einem Internet Service Provider (ISP) verwaltet wird und als Vermittler zwischen Benutzeranforderungen und DNS-Namenserver fungiert. Wenn Sie einen Browser öffnen und einen Domänennamen in die Adresszeile eingeben, geht die Abfrage zuerst an einen DNS-Auflöser. Der Auflöser kommuniziert mit DNS-Namenservern, um die IP-Adresse für die entsprechende Ressource abzurufen, wie zum Beispiel einen Webserver. Ein DNS-

Auflöser wird auch als rekursiver Namenserver bezeichnet, da er sendet Anfragen an eine Reihe autoritativer DNS-Namenserver sendet, bis er die Antwort erhält (in der Regel eine IP-Adresse), die er an das Gerät eines Benutzers zurückgibt, z. B. einen Webbrowser auf einem Laptop.

Domain Name System (DNS)

Ein weltweites Netzwerk von Servern, über die Computer, Smartphones, Tablets und anderen IP-Geräte miteinander kommunizieren können. Das Domain Name System übersetzt leicht verständlichen Namen wie example.com in Zahlen, auch bekannt als IP-Adressen, die es Computern ermöglichen, einander im Internet zu finden.

Siehe auch IP address.

Gehostete Zone

Ein Container für Datensätze, die Informationen darüber enthalten, wie Sie den Datenverkehr zu einer Domäne (z. B. example.com) und allen ihren Subdomänen (z. B. www.example.com, retail.example.com und seattle.accounting.example.com) weiterleiten möchten. Eine gehostete Zone trägt denselben Namen wie die entsprechende Domäne.

Die gehostete Zone für example.com kann beispielsweise einen Datensatz enthalten, der Informationen über die Weiterleitung von Datenverkehr für www.example.com an einen Webserver mit der IP-Adresse 192.0.2.243 enthält, sowie einen Datensatz mit Informationen über die Weiterleitung von E-Mail-Nachrichten für example.com an zwei E-Mail-Server, nämlich mail1.example.com und mail2.example.com. Jeder E-Mail-Server erfordert auch seinen eigenen Datensatz.

Siehe auch record (DNS record).

IP-Adresse

Eine Zahl, die einem Gerät im Internet zugeordnet istwie einem Laptop, Smartphone oder Webserverund mit der das Gerät mit anderen Geräten im Internet kommunizieren kann. IP-Adressen haben eines der folgenden Formate:

- Format des Internetprotokolls, Version 4 (IPv4), z. B. 192.0.2.44
- Internetprotokollformat, Version 6 (IPv6), z. B. 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345

Route IPv4 IPv6 53 unterstützt sowohl als auch Adressen für die folgenden Zwecke:

- Sie können Datensätze mit dem Typ A für IPv4 Adressen oder dem Typ AAAA für IPv6 Adressen erstellen.

- Sie können Integritätsprüfungen erstellen, die Anfragen entweder an IPv4 oder an IPv6 Adressen senden.
- Befindet sich ein DNS-Resolver in einem IPv6 Netzwerk, kann er entweder IPv4 oder verwenden, IPv6 um Anfragen an Route 53 zu senden.

Namenserver

Server im Domain Name System (DNS), die helfen, Domänennamen in IP-Adressen zu übersetzen, die Computer zur Kommunikation miteinander verwenden. Namenserver sind entweder rekursive Namenserver (auch bekannt als DNS resolver) oder authoritative name server.

Einen Überblick darüber, wie das DNS Datenverkehr an Ihre Ressourcen weiterleitet, einschließlich der Rolle von Route 53 im Prozess, finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Privates DNS

Eine lokale Version des Domain Name Systems (DNS), mit der Sie den Traffic für eine Domain und ihre Subdomains an EC2 Amazon-Instances innerhalb einer oder mehrerer Amazon Virtual Private Clouds (VPCs) weiterleiten können. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.

-Datensatz (DNS-Datensatz)

Ein Objekt in einer gehosteten Zone, die Sie verwenden, um zu definieren, wie Datenverkehr für eine Domäne oder Subdomäne weitergeleitet werden soll. Sie können beispielsweise Datensätze erstellen, die den Datenverkehr für example.com und www.example.com an einen Webserver mit der IP-Adresse 192.0.2.234 weiterleiten.

Weitere Informationen zu Datensätzen, einschließlich Informationen über Funktionen, die von Route-53-spezifischen Datensätzen bereitgestellt werden, finden Sie unter Konfigurieren von Amazon Route 53 als DNS-Service.

Rekursiver Namenserver

Siehe DNS resolver.

Wiederverwendbare Delegationssätze

Eine Gruppe aus vier autoritativen Namenservern, die Sie mit mehr als einer gehosteten Zone verwenden können. Standardmäßig weist Route 53 eine zufällige Auswahl von Namenservern

für jede neue gehostete Zone zu. Um die Migration von DNS-Services in Route 53 für eine große Anzahl von Domänen zu vereinfachen, können Sie einen wiederverwendbaren Delegationssatz erstellen und anschließend den wiederverwendbaren Delegationssatz neuen gehosteten Zonen zuordnen. (Sie können die Namenserver, die mit einer vorhandenen gehosteten Zone verknüpft sind, nicht mehr ändern.)

Sie erstellen einen wiederverwendbaren Delegationssatz und verknüpfen ihn programmgesteuert mit einer gehosteten Zone. Die Verwendung der Route-53-Konsole wird nicht unterstützt. Weitere Informationen finden Sie unter CreateHostedZoneund CreateReusableDelegationSetin der Amazon Route 53 API-Referenz. Dieselbe Funktion ist auch in den AWS SDKsAWS Command Line Interface, und verfügbar AWS Tools for Windows PowerShell.

Routing-Richtlinie

Eine Einstellung für Datensätze, die bestimmt, wie Route 53 DNS-Abfragen beantwortet. Route 53 unterstützt die folgenden Routing-Richtlinien:

- Einfache Routing-Richtlinie – wird zum Weiterleiten von Internetdatenverkehr an eine einzelne Ressource verwendet, die eine bestimmte Funktion für Ihre Domäne übernimmt, beispielsweise ein Webserver, der für die Inhalte für die Website example.com zuständig ist.
- Failover-Routing-Richtlinie – wird verwendet, wenn Sie ein Aktiv-Passiv-Failover konfigurieren möchten.
- Geolocation-Routing-Richtlinie – wird verwendet, wenn Sie den Internetdatenverkehr auf Basis des Standorts Ihrer Benutzer an Ihre Ressourcen weiterleiten möchten.
- Routing-Richtlinie auf der Grundlage der geografischen Nähe – wird verwendet, wenn Sie den Datenverkehr auf der Basis des Standorts Ihrer Ressourcen weiterleiten möchten und optional den Datenverkehr von Ressourcen an einem Standort zu Ressourcen an einem anderen Standort verschieben möchten.
- Latenz-Routing-Richtlinie – wird verwendet, wenn Sie Ressourcen an mehreren Standorten haben und Datenverkehr zu der Ressource leiten möchten, die die niedrigste Latenz bietet.
- IP-basierte Routing-Richtlinie: Wird verwendet, wenn Sie den Datenverkehr auf Basis des Standorts Ihrer Benutzer weiterleiten möchten und die IP-Adressen haben, von denen der Datenverkehr stammt.
- Mehrwertige Antwort-Routing-Richtlinie – wird verwendet, wenn Sie möchten, dass Route 53 mit bis zu acht zufällig ausgewählten und fehlerfreien Datensätzen auf DNS-Abfragen antwortet.
- Gewichtete Routing-Richtlinie – wird verwendet, um Datenverkehr in festgelegten Proportionen zu mehreren Ressourcen weiterzuleiten.

Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Subdomäne

Ein Domänenname, dem eine oder mehrere Bezeichnungen vor dem registrierten Domänennamen vorangestellt sind. Wenn Sie beispielsweise den Domänennamen example.com registriert haben, ist www.example.com eine Subdomäne. Wenn Sie die gehostete Zone accounting.example.com für die Domäne example.com erstellen, dann ist seattle.accounting.example.com eine Subdomäne.

Um den Datenverkehr für eine Subdomäne weiterzuleiten, erstellen Sie einen Datensatz mit dem gewünschten Namen, z. B. www.example.com, und geben die entsprechenden Werte wie die IP-Adresse eines Webservers an.

TTL (Time to Live, Gültigkeitsdauer)

Die Zeitdauer in Sekunden, die ein DNS-Resolver die Werte für einen Datensatz zwischenspeichern soll, bevor eine weitere Anforderung an Route 53 gesendet wird, um die aktuellen Werte für diesen Datensatz abzufragen. Wenn der DNS-Auflöser eine andere Anforderung für dieselbe Domäne erhält, bevor die TTL abgelaufen ist, gibt der Auflöser den zwischengespeicherten Wert zurück.

Eine längere TTL senkt die Route-53-Gebühren, die zum Teil auf der Anzahl der DNS-Abfragen basiert, die von Route 53 beantwortet werden. Eine kürzere TTL reduziert die Zeitdauer, in der DNS-Resolver Datenverkehr an ältere Ressourcen leitet, nachdem Sie die Werte in einem Datensatz geändert haben, z. B. indem Sie die IP-Adresse für den Webserver für www.example.com ändern.

Konzepte für Steuer- und Datenebene

Im Folgenden finden Sie eine Übersicht über die Konzepte im Zusammenhang mit der Aufteilung der Funktionalität von Amazon Route 53 in eine Steuer- und Datenebene. Route 53 Service enthält – wie die meisten AWS-Services– eine Steuerebene, mit der Sie Verwaltungsvorgänge wie das Erstellen, Aktualisieren und Löschen von Ressourcen ausführen können, sowie eine Datenebene, die die Kernfunktionalität des Dienstes bereitstellt. Während beide Funktionalitäten zuverlässig sind, sind die Steuerebenen auf Datenkonsistenz optimiert, während die Datenebenen auf Verfügbarkeit optimiert sind. Das widerstandsfähige Design der Datenebene ermöglicht es ihr, die Verfügbarkeit auch bei seltenen störenden Ereignissen aufrechtzuerhalten, bei denen die Steuerebene möglicherweise nicht verfügbar wird. Aus diesem Grund empfehlen wir die Verwendung von Funktionen der Datenebene, wenn die Verfügbarkeit wichtig ist.

Für öffentliche und private DNS- und Zustandsprüfungen von Route 53 befindet sich die Kontrollebene in der US-East-1 AWS-Region und die Datenebenen sind weltweit verteilt.

Amazon Route 53 ist wie folgt in Steuer- und Datenebenen unterteilt:

- Bei öffentlichem und privatem DNS von Route 53 besteht die Kontrollebene aus der Route 53 APIs, mit der Sie DNS-Einträge verwalten können, einschließlich Route 53 und Traffic Flow. APIs Die Route 53-Konsole befindet sich in den US-East-1. Wenn jedoch festgestellt wird AWS-Region AWS , dass in dieser Region eine Beeinträchtigung vorliegt, wird die Route 53-Konsole von der US-West-2 bedient. AWS-Region Die Datenebene ist der maßgebliche DNS-Dienst, der über 200 Points-of-Presence-Standorte (PoP) erstreckt und DNS-Anfragen basierend auf Ihren gehosteten Zonen und Daten der Zustandsprüfung beantwortet.
- Für Route 53-Zustandsprüfungen besteht die Kontrollebene aus der Route 53 APIs , mit der Sie Zustandsprüfungen erstellen, aktualisieren und löschen können. Die Route 53-Zustandsprüfungskonsole befindet sich in der Region US-East-1. Wenn jedoch festgestellt wird AWS-Region AWS , dass in dieser Region eine Beeinträchtigung vorliegt, wird die Route 53-Konsole für die Zustandsprüfungen von der US-West-2 bedient. AWS-Region Die Datenebene ist der global verteilte Dienst, der Zustandsprüfungen durchführt, die Ergebnisse aggregiert und an die Datenebenen des öffentlichen und privaten DNS der Route 53 und AWS Global Accelerator liefert.
- Für Route 53 VPC Resolver besteht die Kontrollebene aus dem VPC Resolver, mit dem Sie Amazon VPC-Einstellungen APIs , Resolver-Regeln, Abfrageprotokollierungsrichtlinien und DNS-Firewall-Richtlinien verwalten können. Die Datenebene ist der DNS-Resolver-Dienst, der DNS-Abfragen in Ihrer VPC beantwortet, Endpunkte, die Abfragen an andere Resolver weiterleiten, und die DNS-Firewall-Datenebene, die Richtlinien zum Filtern von DNS-Abfragen anwendet. VPC Resolver ist ein regionaler Dienst, dessen Steuerungs- und Datenebenen jeweils unabhängig voneinander ausgeführt werden. AWS-Region
- Domainregistrierungen der Route 53 werden nur auf der Steuerebene in den AWS-Region us-east-1 verwaltet.

Weitere Informationen zu Datenebenen, Kontrollebenen und dazu, wie Services AWS entwickelt werden, um Hochverfügbarkeitsziele zu erreichen, finden Sie im paper Statische Stabilität mithilfe von Availability Zones in der Amazon Builders' Library.

Konzepte für Zustandsprüfungen

Im Folgenden finden Sie eine Übersicht über die Konzepte im Zusammenhang mit der Zustandsprüfung von Amazon Route 53.

- DNS failover
- endpoint
- health check

DNS-Failover

Eine Methode für die Weiterleitung weg von fehlerhaften Ressourcen und hin zu fehlerfreien Ressourcen. Wenn Sie mehr als eine Ressource haben, die dieselbe Funktion ausführt z. B. mehr als einen Webserver oder E-Mail-Server, können Sie Route-53-Zustandsprüfungen konfigurieren, um den Zustand Ihrer Ressourcen und Konfiguration zu überprüfen, und festlegen, dass Datensätze in Ihrer gehosteten Zone den Datenverkehr nur an ordnungsgemäß funktionierende Ressourcen weiterleiten.

Weitere Informationen finden Sie unter Konfigurieren von DNS Failover.

Endpunkt

Die Ressource, z. B. ein Webserver oder ein E-Mail-Server, für die Sie eine Zustandsprüfung konfigurieren, um den Zustand zu überwachen. Sie können einen Endpunkt nach IPv4 Adresse (192.0.2.243), nach IPv6 Adresse (2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) oder nach Domainnamen (example.com) angeben.

> **Note**
>
> Sie können auch Integritätsprüfungen erstellen, die den Status anderer Integritätsprüfungen oder den Alarmstatus eines Alarms überwachen. CloudWatch

Zustandsprüfung

Eine Route-53-Komponente, mit der Sie Folgendes ausführen können:

- Überwachen, ob ein festgelegter Endpunkt, wie z. B. ein Webserver, betriebsbereit ist
- Optional können Sie benachrichtigt werden, wenn ein Endpunkt fehlerhaft ist
- Sie können DNS-Failover konfigurieren, sodass der Internetdatenverkehr von einer fehlerhaften Ressource an eine fehlerfreie Ressource umgeleitet wird

Weitere Informationen zum Erstellen und Verwenden von Zustandsprüfungen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

Erste Schritte mit Amazon Route 53

In den folgenden Themen dieses Handbuchs finden Sie Informationen zu den ersten Schritten mit Amazon Route 53:

- Amazon Route 53 einrichten, in dem erklärt wird, wie Sie sich registrieren AWS, wie Sie den Zugriff auf Ihr AWS Konto sichern und wie Sie den programmatischen Zugriff auf Route 53 einrichten
- Erste Schritte mit Amazon Route 53: Beschreibt, wie Sie einen Domainnamen registrieren, wie Sie einen Amazon-S3-Bucket erstellen und zum Hosten einer statischen Website konfigurieren und wie Sie den Internetdatenverkehr an die Website weiterleiten

Zugriff auf Amazon Route 53

Sie können wie folgt auf Amazon Route 53 zugreifen:

- AWS-Managementkonsole— Die Verfahren in diesem Handbuch erläutern, wie Sie mit AWS-Managementkonsole dem Aufgaben ausführen können.
- AWS SDKs— Wenn Sie eine Programmiersprache verwenden, die ein SDK für AWS bereitstellt, können Sie ein SDK für den Zugriff auf Route 53 verwenden. SDKs vereinfachen Sie die Authentifizierung, lassen sich problemlos in Ihre Entwicklungsumgebung integrieren und bieten Sie einfachen Zugriff auf Route 53-Befehle. Weitere Informationen finden Sie unter Tools für Amazon Web Services.
- Route-53-API: Wenn Sie eine Programmiersprache verwenden, für die kein SDK verfügbar ist, finden Sie in der Amazon-Route-53-API-Referenz Informationen zu API-Aktionen und zur Ausführung von API-Anfragen.
- AWS Command Line Interface – Weitere Informationen finden Sie unter Einrichtung der AWS Command Line Interface im AWS Command Line Interface -Benutzerhandbuch.
- AWS Tools for Windows PowerShell – Weitere Informationen finden Sie unter Einrichten von AWS Tools for Windows PowerShell im AWS -Tools für PowerShell -Benutzerhandbuch.

AWS Identitäts- und Zugriffsverwaltung

Amazon Route 53 ist in AWS Identity and Access Management (IAM) integriert, einen Service, mit dem Ihr Unternehmen Folgendes tun kann:

- Erstellen Sie Benutzer und Gruppen unter dem Konto Ihrer Organisation AWS

- Teilen Sie Ihre AWS Kontoressourcen ganz einfach mit den Benutzern im Konto
- Zuweisen eindeutiger Sicherheitsanmeldeinformationen zu jedem Benutzer
- Genaue Kontrolle des Zugriffs jedes Benutzers auf Dienste und Ressourcen

Sie können beispielsweise IAM mit Route 53 verwenden, um zu steuern, welche Benutzer in Ihrem AWS Konto eine neue gehostete Zone erstellen oder Datensätze ändern können.

Allgemeine Informationen zu IAM finden Sie unter:

- Identity and Access Management in Amazon Route 53
- Identity and Access Management (IAM)
- IAM Benutzerhandbuch

Amazon-Route-53-Preise und -Abrechnung

Wie bei anderen AWS Produkten gibt es keine Verträge oder Mindestverpflichtungen für die Nutzung von Amazon Route 53. Sie zahlen nur für die gehosteten Zonen, die Sie konfigurieren, und die Anzahl der von Route 53 beantworteten DNS-Abfragen. Weitere Informationen dazu finden Sie unter Amazon Route 53 – Preise.

Informationen zur Abrechnung von AWS Dienstleistungen, einschließlich der Anzeige Ihrer Rechnung und der Verwaltung Ihres Kontos und Ihrer Zahlungen, finden Sie im AWS Billing Benutzerhandbuch.

Route 53 mit einem AWS SDK verwenden

AWS Software Development Kits (SDKs) sind für viele beliebte Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK für Go	AWS SDK für Go Code-Beispiele

SDK-Dokumentation	Codebeispiele
AWS SDK für Java	AWS SDK für Java Code-Beispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Code-Beispiele
AWS SDK für Kotlin	AWS SDK für Kotlin Code-Beispiele
AWS SDK für .NET	AWS SDK für .NET Code-Beispiele
AWS SDK für PHP	AWS SDK für PHP Code-Beispiele
AWS -Tools für PowerShell	AWS -Tools für PowerShell Code-Beispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Code-Beispiele
AWS SDK für Ruby	AWS SDK für Ruby Code-Beispiele
AWS SDK für Rust	AWS SDK für Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK für Swift	AWS SDK für Swift Code-Beispiele

Spezifische Beispiele für Route 53 finden Sie unter Codebeispiele für Route 53 mit AWS SDKs.

> **Beispiel für die Verfügbarkeit**
>
> Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Erste Schritte mit Amazon Route 53

Beginnen Sie mit der Registrierung einer Domäne bei Amazon Route 53 und der Konfiguration von Route 53, um DNS-Abfragen zu beantworten. Das erste Tutorial hostet eine statische Website in einem offenen Amazon S3 S3-Bucket, und das zweite Tutorial verwendet CloudFront Amazon-Distribution, um die Website mit SSL/TLS bereitzustellen.

Geschätzte Kosten

- Es gibt eine Jahresgebühr für die Registrierung einer Domäne, zwischen 9 und mehreren hundert Dollar, je nach Top-Level-Domain wie beispielsweise .com. Weitere Informationen finden Sie unter Route 53-Preise für die Domänenregistrierung. Diese Gebühr kann nicht erstattet werden.
- Wenn Sie eine Domäne registrieren, erstellen wir automatisch eine gehostete Zone, die denselben Namen wie die Domäne hat. Sie verwenden die gehostete Zone, um anzugeben, wohin Route 53 den Datenverkehr für Ihre Domäne leiten soll.
- In diesem Tutorial erstellen Sie einen Amazon S3-Bucket und laden eine Beispiel-Webseite hoch. Wenn Sie ein neuer AWS Kunde sind, können Sie kostenlos mit Amazon S3 beginnen. Wenn Sie bereits AWS Kunde sind, richten sich die Gebühren danach, wie viele Daten Sie speichern, nach der Anzahl der Anfragen für Ihre Daten und nach der Menge der übertragenen Daten. Weitere Informationen finden Sie unter Amazon S3 – Preise.
- CloudFront Die Gebühren basieren auf der Anzahl der Anfragen für Ihre Daten, der Anzahl der von Ihnen verwendeten Edge-Standorte und der Menge der übertragenen Daten. Weitere Informationen finden Sie unter CloudFront – Preise.

Themen

Amazon Route 53 einrichten

Die Übersicht und die Verfahren in diesem Abschnitt helfen Ihnen bei den ersten Schritten AWS.

Themen

- Erstellen eines Benutzers mit Administratorzugriff
- Tools herunterladen

Melde dich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung -Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center - Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center - Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center - Benutzerhandbuch.

Tools herunterladen

Das AWS-Managementkonsole beinhaltet eine Konsole für Amazon Route 53, aber wenn Sie programmgesteuert auf die Dienste zugreifen möchten, lesen Sie Folgendes:

- Der API-Leitfaden dokumentiert die von den Services unterstützten Operationen und stellt Links zu den zugehörigen SDK- und CLI-Dokumentationen bereit:
  - API-Referenz für Amazon Route 53
- Um eine API aufzurufen, ohne sich um Details auf niedriger Ebene kümmern zu müssen, wie z. B. das Zusammenstellen von rohen HTTP-Anfragen, können Sie ein SDK verwenden. AWS AWS SDKs Sie stellen Funktionen und Datentypen bereit, die die Funktionalität von Diensten zusammenfassen. AWS Informationen zum Herunterladen eines AWS SDK und zum Zugriff auf Installationsanweisungen finden Sie auf der entsprechenden Seite:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Eine vollständige Liste von AWS SDKs finden Sie unter Tools für Amazon Web Services.
- Sie können die AWS Command Line Interface (AWS CLI) verwenden, um mehrere AWS Dienste von der Befehlszeile aus zu steuern. Sie können Ihre Befehle auch mithilfe von Skripts automatisieren. Weitere Informationen finden Sie unter AWS Command Line Interface.
- AWS Tools for Windows PowerShell unterstützt diese AWS Dienste. Weitere Informationen finden Sie in der AWS -Tools für PowerShell -Cmdlet-Referenz.

Verwenden Sie Ihre Domain für eine statische Website in einem Amazon S3 Bucket

Dieses Tutorial zeigt Ihnen, wie Sie Amazon Route 53 verwenden, um DNS-Verkehr für Ihre Domain an einen Amazon Simple Storage Service-Bucket weiterzuleiten, der eine statische Website hostet. Sie erstellen Alias-Einträge, die Ihre Domain auf den Endpunkt der S3-Website verweisen.

Dieses Tutorial ist Teil eines vollständigen Workflows zur Einrichtung einer statischen Website. Allgemeine Informationen zur Weiterleitung von Datenverkehr an einen beliebigen S3-Bucket finden Sie unterWeiterleiten von Datenverkehr an eine Website, die in einem Amazon-S3-Bucket gehostet wird..

Wenn Sie fertig sind, können Besucher mit Ihrem benutzerdefinierten Domainnamen auf Ihre statische Website zugreifen.

> **Note**
>
> Sie können auch eine vorhandene Domäne in Route 53 übertragen, aber der Prozess ist komplex und zeitaufwendiger als eine neue Domänenregistrierung. Weitere Informationen finden Sie unter Übertragen der Registrierung für eine Domain an Amazon Route 53.

Voraussetzungen

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Führen Sie die Schritte unter Amazon Route 53 einrichten aus.
- Registrieren Sie einen Domainnamen mit Amazon Route 53. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.
- Konfigurieren Sie einen Amazon Simple Storage Service-Bucket für statisches Website-Hosting. Vollständige Anweisungen finden Sie unter Tutorial: Konfiguration einer statischen Website mithilfe einer benutzerdefinierten Domain, die bei Route 53 registriert ist, im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn Sie das Amazon Simple Storage Service-Tutorial abgeschlossen haben, haben Sie:

- Amazon S3 S3-Buckets, die für das Hosting und die Weiterleitung von Websites konfiguriert sind (bei Verwendung der www-Subdomain)
- Der Inhalt der Website wurde in Ihren Bucket hochgeladen
- Öffentlicher Zugriff, der für Ihren Website-Bucket konfiguriert ist

Schritt 1: Leiten Sie den DNS-Verkehr für Ihre Domain an Ihren Website-Bucket weiter

Nachdem Sie nun einen Amazon Simple Storage Service-Bucket für statisches Website-Hosting konfiguriert haben, verwenden Sie Amazon Route 53, um den DNS-Verkehr für Ihre Domain an den Bucket weiterzuleiten. Auf diese Weise können Besucher mit Ihrem benutzerdefinierten Domainnamen auf Ihre Website zugreifen.

So leiten Sie den Datenverkehr an Ihre Website

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

   > **Note**
   >
   > Als Sie Ihre Domain registriert haben, hat Amazon Route 53 automatisch eine gehostete Zone mit demselben Namen erstellt. Eine gehostete Zone enthält Informationen darüber, wie Sie möchten, dass Route 53 den Datenverkehr für die Domäne weiterleitet.

3. Wählen Sie in der Liste der gehosteten Zonen den Namen Ihrer Domäne aus.
4. Wählen Sie Create record (Datensatz erstellen).
5. Geben Sie die folgenden Werte an:

   Datensatzname

   Lassen Sie das Feld leer, um einen Eintrag für Ihre Root-Domain zu erstellen.

   Datensatztyp

   Wählen Sie A - Leitet Traffic an eine IPv4 Adresse und einige AWS Ressourcen weiter.

   Alias

   Schalten Sie Alias ein.

   Datenverkehr weiterleiten an

   Wählen Sie Alias für den Endpunkt der S3-Website.

   Wählen Sie die Region aus, in der Sie Ihren S3-Bucket erstellt haben.

Wählen Sie Ihren S3-Bucket aus. Der Bucket-Name sollte mit dem Namen Ihrer Domain übereinstimmen. In der Liste wird der Bucket-Name zusammen mit dem Amazon S3 S3-Website-Endpunkt für die Region angezeigt, in der der Bucket erstellt wurde, `s3-website-us-west-1.amazonaws.com (example.com)` z. B.

Wenn Ihr Bucket nicht in der Liste erscheint, geben Sie den Amazon S3 S3-Website-Endpunkt für die Region ein, in der der Bucket erstellt wurde, **`s3-website-us-west-2.amazonaws.com`** z. B. Eine vollständige Liste der Amazon-S3-Website-Endpunkte finden Sie unter Amazon-S3-Website-Endpunkte.

Evaluate Target Health

Übernehmen Sie den Standardwert No.

6. Wählen Sie Create records (Datensätze erstellen).

So fügen Sie Ihrer Subdomäne () einen Alias-Datensatz hi (**`www.example.com`**)

Wenn Sie einen Bucket für Ihre Subdomain erstellt haben, fügen Sie auch einen Aliasdatensatz hinzu.

1. Wählen Sie Datensatz erstellen.
2. Geben Sie die folgenden Werte an:

Datensatzname

Geben Sie **`www`** ein.

Datensatztyp

Wählen Sie A - Leitet den Traffic an eine IPv4 Adresse und einige AWS Ressourcen weiter.

Alias

Schalten Sie Alias ein.

Datenverkehr weiterleiten an

Wählen Sie Alias für den Endpunkt der S3-Website.

Wählen Sie die Region aus, in der Sie Ihren S3-Bucket erstellt haben.

Wählen Sie Ihren S3-Bucket für die Subdomain aus, zum Beispiel. `s3-website-us-west-2.amazonaws.com (www.example.com)`

Evaluate Target Health

Übernehmen Sie den Standardwert No.

3. Wählen Sie Create records (Datensätze erstellen).

Schritt 2: Testen Sie Ihre Website

Um zu überprüfen, ob die Website ordnungsgemäß funktioniert, öffnen Sie einen Webbrowser und navigieren Sie zu den folgenden Seiten URLs:

- http://*your-domain-name*, zum Beispiel `example.com` — Zeigt das Indexdokument im *your-domain-name* Bucket an
- http://www. *your-domain-name*Beispiel: `www.example.com` — Leitet Ihre Anfrage an den *your-domain-name* Bucket weiter

In einigen Fällen müssen Sie möglicherweise den Cache löschen, um das erwartete Verhalten zu sehen.

Ausführlichere Informationen über das Weiterleiten von Internetdatenverkehr finden Sie unter Konfigurieren von Amazon Route 53 als DNS-Service. Hinweise zur Weiterleitung Ihres Internetverkehrs zu AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

> **Note**
>
> Amazon S3 unterstützt keinen HTTPS-Zugriff auf die Website. Wenn Sie HTTPS verwenden möchten, können Sie Amazon verwenden, CloudFront um eine statische Website bereitzustellen, die auf Amazon S3 gehostet wird. Weitere Informationen finden Sie unter Verwenden Sie eine CloudFront Amazon-Distribution, um eine statische Website bereitzustellen.

Verwenden Sie eine CloudFront Amazon-Distribution, um eine statische Website bereitzustellen

Dieses Tutorial zeigt Ihnen, wie Sie Amazon Route 53 verwenden, um DNS-Verkehr für Ihre Domain an CloudFront Amazon-Distributionen weiterzuleiten, die eine statische Website bedienen. Sie erstellen Alias-Einträge, die Ihre Domain und Subdomain auf Distributionen verweisen. CloudFront

Dieses Tutorial ist Teil eines vollständigen Workflows zur Einrichtung statischer Websites. Allgemeine Informationen zur Weiterleitung von Datenverkehr an beliebige CloudFront Distributionen finden Sie unterWeiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

Wenn Sie fertig sind, können Besucher über Ihren benutzerdefinierten Domainnamen mit HTTPS-Sicherheit von auf Ihre Website zugreifen CloudFront.

Voraussetzungen

Bevor Sie beginnen, führen Sie die folgenden Schritte aus:

- Führen Sie die Schritte unter Amazon Route 53 einrichten aus.
- Registrieren Sie einen Domainnamen mit Amazon Route 53. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.
- Erstellen Sie mit Amazon CloudFront und Amazon Simple Storage Service eine sichere statische Website. Vollständige Anweisungen finden Sie unter Erste Schritte mit einer sicheren statischen Website im Amazon CloudFront Developer Guide.

Wenn Sie das CloudFront Amazon-Tutorial abgeschlossen haben, haben Sie:

- Ein SSL/TLS Zertifikat für Ihre Domain in AWS Certificate Manager
- Amazon S3 S3-Buckets, die für das Hosting und die Weiterleitung von Websites konfiguriert sind
- CloudFront Distributionen sowohl für Ihre Root-Domain als auch für Ihre Subdomain

Schritt 1: Leiten Sie den DNS-Verkehr für Ihre Domain an Ihre Distribution weiter CloudFront

Nachdem Sie nun CloudFront Amazon-Distributionen für Ihre Website haben, verwenden Sie Amazon Route 53, um den DNS-Verkehr für Ihre Domain an die Distributionen weiterzuleiten. Dadurch können Besucher mit Ihrem benutzerdefinierten Domainnamen auf Ihre Website zugreifen.

Weitere Informationen zur Weiterleitung von Traffic an CloudFront Distributionen finden Sie unterWeiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

So leiten Sie den Datenverkehr an Ihre Website

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

   > **Note**
   >
   > Als Sie Ihre Domain registriert haben, hat Amazon Route 53 automatisch eine gehostete Zone mit demselben Namen erstellt. Eine gehostete Zone enthält Informationen darüber, wie Sie möchten, dass Route 53 den Datenverkehr für die Domäne weiterleitet.

3. Wählen Sie in der Liste der gehosteten Zonen den Namen Ihrer Domäne aus.
4. Wählen Sie Create record (Datensatz erstellen).
5. Geben Sie die folgenden Werte an:

   Datensatzname

   Geben **www** Sie für Ihren Subdomain-Datensatz ein.

   Datensatztyp

   Wählen Sie A - Leitet Traffic an eine IPv4 Adresse und einige AWS Ressourcen weiter.

   Alias

   Schalten Sie Alias ein.

   Datenverkehr weiterleiten an

   Wählen Sie Alias für die CloudFront Verteilung aus.

   Wählen Sie die Region us-east-1.

Wählen Sie Ihre Distribution CloudFront . Der Name der Distribution sollte mit dem Namen übereinstimmen, der in der Spalte Domainname in der CloudFront Konsole angezeigt wird, `dddjjjkkk.cloudfront.net` z. B.

Evaluate Target Health

Übernehmen Sie den Standardwert No.

6. Wählen Sie Create records (Datensätze erstellen).

So fügen Sie Ihrer Stamm-Domäne einen Aliasdatensatz hinzu (**`example.com`**)

Fügen Sie auch einen Aliaseintrag für Ihre Stammdomain hinzu, sodass er auf die CloudFront Distribution verweist, zu der der Traffic umgeleitet wird`www.example.com`.

1. Wählen Sie Datensatz erstellen.
2. Geben Sie die folgenden Werte an:

   Datensatzname

   Lassen Sie das Feld leer, um einen Eintrag für Ihre Root-Domain zu erstellen.

   Datensatztyp

   Wählen Sie A - Leitet Traffic an eine IPv4 Adresse und einige AWS Ressourcen weiter.

   Alias

   Schalten Sie Alias ein.

   Datenverkehr weiterleiten an

   Wählen Sie Alias für die CloudFront Verteilung aus.

   Wählen Sie die Region us-east-1.

   Wählen Sie Ihre CloudFront Root-Domain-Distribution.

   Evaluate Target Health

   Übernehmen Sie den Standardwert No.

3. Wählen Sie Create records (Datensätze erstellen).

Schritt 2: Testen Sie Ihre Website

Um zu überprüfen, ob die Website ordnungsgemäß funktioniert, öffnen Sie einen Webbrowser und navigieren Sie zu den folgenden Seiten URLs:

- https://www. *your-domain-name*, zum Beispiel, `www.example.com` — Zeigt das Indexdokument im *www.your-domain-name* Bucket an
- https://*your-domain-name*zum Beispiel, `example.com` — Leitet Ihre Anfrage an den *www.your-domain-name* Bucket weiter

In einigen Fällen müssen Sie möglicherweise den Cache löschen, um das erwartete Verhalten zu sehen.

Ausführlichere Informationen über das Weiterleiten von Internetdatenverkehr finden Sie unter Konfigurieren von Amazon Route 53 als DNS-Service. Hinweise zur Weiterleitung Ihres Internetverkehrs zu AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Integration in andere -Services

Sie können Amazon Route 53 mit anderen AWS Services integrieren, um Anfragen zu protokollieren, die an die Route 53-API gesendet werden, den Status Ihrer Ressourcen zu überwachen und Ihren Ressourcen Tags zuzuweisen. Darüber hinaus können Sie mithilfe von Route 53 Internetdatenverkehr an Ihre AWS -Ressourcen weiterleiten.

Themen

Protokollierung, Überwachung und Markieren

AWS CloudTrail

Amazon Route 53 ist integriert AWS CloudTrail, ein Service, der Informationen zu jeder Anfrage erfasst, die von Ihrem AWS Konto an die Route 53-API gesendet wird. Sie können anhand der Informationen in den CloudTrail Protokolldateien feststellen, welche Anfragen an Route 53 gestellt wurden, von welcher Quell-IP-Adresse jede Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde usw.

Weitere Informationen finden Sie unter Protokollieren von Amazon Route 53-API-Aufrufen mit AWS CloudTrail.

Amazon CloudWatch

Sie können Amazon verwenden CloudWatch , um den Status — fehlerfrei oder ungesund — Ihrer Route 53-Zustandsprüfungen zu überwachen. Zustandsprüfungen überwachen den Zustand und die Leistung Ihrer Webanwendungen, Webserver und anderer Ressourcen. In regelmäßigen Intervallen, die Sie festlegen, sendet Route 53 automatisierte Anfragen über das Internet an Ihre Anwendung, den Server oder andere Ressourcen, um sicherzustellen, dass sie erreichbar, verfügbar und funktionsfähig sind.

Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

Tag Editor

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen, einschließlich Route 53-Domains, gehosteten Zonen und Zustandsprüfungen. Jedes Tag besteht aus einem Schlüssel

und einem Wert, die Sie beide selbst definieren. Beispielsweise können Sie ein Tag zu einer Domänenregistrierung zuweisen, die den Schlüssel "Kunde" und den Wert "Beispielfirma" hat. Sie können Tags für eine Vielzahl von Zwecken verwenden. Häufig werden sie verwendet, um Ihre AWS Kosten zu kategorisieren und nachzuverfolgen.

Weitere Informationen finden Sie unter Amazon-Route-53-Ressourcen-Markierung.

Weiterleitung des Datenverkehrs an andere Ressourcen AWS

Sie können Amazon Route 53 verwenden, um den Verkehr an eine Vielzahl von AWS Ressourcen weiterzuleiten.

Amazon API Gateway

Mit Amazon API Gateway können Sie in jeder Größenordnung etwas erstellen, veröffentlichen, verwalten, überwachen und sichern APIs . Sie können APIs diesen Zugriff AWS oder andere Webdienste sowie in der AWS Cloud gespeicherte Daten erstellen.

Weiterleiten von Datenverkehr mithilfe von Route 53 an eine API Gateway-API. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens.

Amazon CloudFront

Um die Bereitstellung Ihrer Webinhalte zu beschleunigen, können Sie Amazon CloudFront, das AWS Content Delivery Network (CDN), verwenden. CloudFront kann Ihre gesamte Website — einschließlich dynamischer, statischer, gestreamter und interaktiver Inhalte — mithilfe eines globalen Netzwerks von Edge-Standorten bereitstellen. CloudFront leitet Anfragen für Ihre Inhalte an den Edge-Standort weiter, der Ihren Benutzern die niedrigste Latenz bietet. Sie können Route 53 verwenden, um den Traffic für Ihre Domain an Ihre CloudFront Distribution weiterzuleiten. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

Amazon EC2

Amazon EC2 bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können eine EC2 virtuelle Computerumgebung (eine Instance) mithilfe einer vorkonfigurierten Vorlage (einem Amazon Machine Image oder AMI) starten. Wenn Sie eine EC2 Instance starten, EC2 werden das Betriebssystem (Linux oder Microsoft Windows) und zusätzliche im AMI enthaltene Software, wie Webserver- oder Datenbanksoftware, automatisch installiert.

Wenn Sie eine Website hosten oder eine Webanwendung auf einer EC2 Instance ausführen, können Sie den Traffic für Ihre Domain, z. B. example.com, mithilfe von Route 53 an Ihren Server weiterleiten. Weitere Informationen finden Sie unter Traffic an eine EC2 Amazon-Instance weiterleiten.

AWS Elastic Beanstalk

Wenn Sie Anwendungen in der AWS Cloud bereitstellen und verwalten, können Sie Route 53 verwenden, um den DNS-Verkehr für Ihre Domain, z. B. example.com, an eine Elastic Beanstalk-Umgebung weiterzuleiten. AWS Elastic Beanstalk Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an eine AWS Elastic Beanstalk Umgebung.

Elastic Load Balancing

Wenn Sie eine Website auf mehreren EC2 Amazon-Instances hosten, können Sie den Traffic auf Ihre Website mithilfe eines Elastic Load Balancing (ELB) -Load Balancers auf die Instances verteilen. Der ELB-Service skaliert automatisch den Load Balancer, wenn sich der Datenverkehr der Website im Laufe der Zeit ändert. Der Load Balancer überwacht auch den Zustand seiner registrierten Instances und leitet den Datenverkehr nur an ordnungsgemäß funktionierende Instances weiter.

Sie können mithilfe von Route 53 Datenverkehr für Ihre Domäne an Ihren Classic, Application oder Network Load Balancer weiterleiten. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr an einen ELB Load Balancer.

Amazon Lightsail

Amazon Lightsail bietet Rechen-, Speicher- und Netzwerkkapazität und Funktionen zur Bereitstellung und Verwaltung von Websites, Webanwendungen und Datenbanken in der Cloud zu einem niedrigen, kalkulierbaren monatlichen Preis.

Wenn Sie Lightsail verwenden, können Sie den Datenverkehr mithilfe von Route 53 an Ihre Lightsail-Instance weiterleiten. Weitere Informationen finden Sie unterVerwenden von Route 53, um eine Domain auf eine Amazon Lightsail -Instance zu verweisenaus.

Amazon S3

Amazon Simple Storage Service (Amazon S3) stellt sicheren, dauerhaften und hochskalierbaren Objektspeicher in der Cloud bereit. Sie können einen S3-Bucket konfigurieren, um eine statische Website zu hosten, wie z. B. Webseiten und clientseitige Skripts. (S3 unterstützt kein serverseitiges Skripting.) Sie können Route 53 verwenden, um den Datenverkehr an einen Amazon-S3-Bucket weiterzuleiten. Weitere Informationen finden Sie unter den folgenden Themen:

- Weitere Informationen über das Weiterleiten von Datenverkehr an einen Bucket finden Sie unter Weiterleiten von Datenverkehr an eine Website, die in einem Amazon-S3-Bucket gehostet wird..
- Eine detaillierte Anleitung zum Hosten einer statischen Website in einem S3-Bucket finden Sie unter Erste Schritte mit Amazon Route 53.

Amazon Virtual Private Cloud (Amazon VPC)

Über einen Schnittstellen-Endpunkt können Sie eine Verbindung zu Diensten herstellen, die von AWS PrivateLink bereitgestellt werden. Zu diesen Diensten gehören einige AWS Dienste, Dienste, die von anderen AWS Kunden und Partnern selbst gehostet werden VPCs (als Endpunktdienste bezeichnet), und unterstützte AWS Marketplace Partnerdienste.

Sie können Route 53 verwenden, um den Datenverkehr an einen Schnittstellenendpunkt weiterzuleiten. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an einen Amazon-Virtual-Private Cloud-Schnittstellenendpunkt unter Verwendung Ihres Domainnamens.

Amazon WorkMail

Wenn Sie Amazon WorkMail für Ihre geschäftlichen E-Mails verwenden und Route 53 als DNS-Service verwenden, können Sie Route 53 verwenden, um den Verkehr an Ihre WorkMail Amazon-E-Mail-Domain weiterzuleiten. Weitere Informationen finden Sie unter Weiterleitung des Datenverkehrs an Amazon WorkMail.

Weitere Informationen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Format für DNS-Domänennamen

Domänennamen (einschließlich der Namen von Domänen, gehosteten Zonen und Datensätzen) bestehen aus einer Reihe von Bezeichnern, die durch Punkte voneinander getrennt sind. Jeder Bezeichner kann bis zu 63 Byte lang sein. Die Gesamtlänge eines Domänennamens darf 255 Byte (einschließlich der Punkte) nicht überschreiten. Amazon Route 53 unterstützt alle gültigen Domänennamen.

Die Namenskonventionen hängen davon ab, ob Sie einen Domänennamen registrieren oder den Namen einer gehosteten Zone oder eines Datensatzes angeben. Weitere Informationen finden Sie im entsprechenden Thema.

Formatierung der Domänennamen für die Domänennamenregistrierung

Für die Registrierung darf ein Domänenname nur die Zeichen a-z, 0-9 und Bindestrich (-) enthalten. Sie dürfen keinen Bindestrich am Anfang oder Ende eines Bezeichners setzen.

Informationen zum Registrieren eines internationalisierten Domänennamens (IDN) finden Sie unter Formatierung internationalisierter Domänennamen.

Formatierung von Domänennamen für gehostete Zonen und Datensätze

Bei gehosteten Zonen und Datensätzen kann der Domänenname beliebige der folgenden druckbaren ASCII-Zeichen (ohne Leerzeichen) enthalten:

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

Amazon Route 53 speichert alphabetische Zeichen als Kleinbuchstaben (a-z), unabhängig davon, wie Sie sie angeben: als Großbuchstaben, Kleinbuchstaben oder entsprechende Buchstaben in Escape-Zeichen.

Wenn Ihr Domainname eines der folgenden Zeichen enthält, müssen Sie die Zeichen mithilfe von Escape-Codes im Format\ angeben*three-digit octal code*:

- Zeichen 000 bis 040 oktal (0 bis 32 dezimal, 0x00 bis 0x20 hexadezimal)
- Zeichen 177 bis 377 oktal (127 bis 255 dezimal, 0x7F bis 0xFF hexadezimal)
- . (Punkt), Zeichen 056 oktal (46 dezimal, 0x2E hexadezimal) bei Verwendung als Zeichen in einem Domänennamen. Bei Verwendung von . als Trennzeichen zwischen Bezeichnern müssen Sie kein Escape-Zeichen setzen.

Wenn der Domänenname andere Zeichen als a-z, 0-9, Bindestrich (-) oder Unterstrich (_) enthält, geben Route 53-API-Aktionen die Zeichen als Escape-Zeichen zurück. Dies gilt unabhängig davon, ob Sie die Zeichen beim Erstellen der Entität als Zeichen oder als Escape-Zeichen angeben. Die Route 53-Konsole zeigt die Zeichen als Zeichen und nicht als Escape-Zeichen an.

Um eine Liste der ASCII-Zeichen mit den entsprechenden Oktalcodes zu erhalten, führen Sie eine Internetsuche nach „ascii tabelle“ durch.

Um einen internationalisierten Domänennamen (IDN) anzugeben, wandeln Sie den Namen in Punycode um. Weitere Informationen finden Sie unter Formatierung internationalisierter Domänennamen.

Verwendung eines Sternchens (*) im Namen von gehosteten Zonen und Datensätzen

Sie können gehostete Zonen erstellen, und Datensätze, deren Name einen „*“ enthält.

Gehostete Zonen

- Ein „*“ kann nicht im Bezeichner ganz links in einem Domänennamen verwendet werden; zum Beispiel ist „*.beispiel.de“ nicht zulässig.
- Wenn Sie „*“ in anderen Positionen verwenden, wird es von DNS wie ein *-Zeichen (ASCII-42) und nicht als Platzhalter behandelt.

Datensätze

Abhängig von seiner Position im Namen wird das *-Zeichen vom DNS entweder als Platzhalter oder als das *-Zeichen (ASCII 42) behandelt. Bitte beachten Sie die folgenden Einschränkungen bei der Verwendung von „*“ als Platzhalter im Namen eines Datensatzes:

- Das „*“ muss den Bezeichner ganz links in einem Domänennamen ersetzen, z. B. *.beispiel.de oder *.acme.example.com. Wenn Sie „*“ in anderen Positionen verwenden (z. B. prod.*.example.com), wird es von DNS wie ein *-Zeichen (ASCII-42) und nicht als Platzhalter behandelt.
- Das „*“ muss den gesamten Bezeichner ersetzen. Sie können z. B. nicht „*prod.beispiel.de“ oder „prod*.beispiel.de“ angeben.
- Spezifische Domänennamen haben Vorrang. Wenn Sie zum Beispiel Datensätze für *.example.com und acme.example.com erstellen, beantwortet Route 53 DNS-Abfragen für acme.example.com immer mit den Werten im Datensatz acme.example.com.
- Das * gilt für DNS-Abfragen für die Subdomäneneben, die das Sternchen enthält, und alle Subdomänen dieser Subdomäne. Wenn Sie beispielsweise einen Datensatz mit dem Namen *.example.com erstellen, verwendet Route 53 die Werte in diesem Datensatz, um auf DNS-Abfragen für zenith.example.com, acme.zenith.example.com und pinnacle.acme.zenith.example.com zu antworten (wenn es keine Datensätze mit diesen Namen gibt).

  Wenn Sie einen Datensatz mit dem Namen *.example.com erstellen und es keinen Datensatz example.com gibt, antwortet Route 53 auf DNS-Abfragen für example.com mit `NXDOMAIN` (nicht existierende Domäne).

  > **Note**
  >
  > Wenn Sie Route 53 mit verwenden AWS Certificate Manager, beachten Sie, dass ACM-Platzhalterzertifikate nur eine Subdomänenebene schützen. Ein ACM-Zertifikat für *.example.com schützt beispielsweise login.example.com und test.example.com, aber nicht test.login.example.com. Weitere Informationen finden Sie unter Eigenschaften und Einschränkungen von AWS Certificate Manager Zertifikaten.

- Sie können Route 53 so konfigurieren, dass es die gleiche Antwort auf DNS-Abfragen sowohl für alle Subdomänen auf derselben Ebene als auch für den Domänennamen zurückgibt. Beispielsweise können Sie Route 53 so konfigurieren, dass DNS-Abfragen wie zenith.example.com und zenith.example.com unter Verwendung des Datensatzes example.com beantwortet werden. Führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Datensatz für die Domäne, wie z. B. example.com.
2. Erstellen Sie einen Alias-Datensatz für die Subdomäne, wie z. B. *.example.com. Geben Sie den Datensatz, den Sie in Schritt 1 erstellt haben, als Ziel für den Alias-Datensatz ein.

- Sie können „*“ nicht als Platzhalter für Datensätze des Typs „NS“ verwenden.

Formatierung internationalisierter Domänennamen

Wenn Sie einen neuen Domänennamen registrieren oder gehostete Zonen und Datensätze erstellen, können Sie Zeichen aus anderen Alphabeten (z. B. Kyrillisch oder Arabisch) und Zeichen in chinesischer, japanischer oder koreanischer Schrift angeben. Amazon Route 53 speichert diese internationalisierten Domainnamen (IDNs) in Punycode, der Unicode-Zeichen als ASCII-Zeichenketten darstellt.

Wenn Sie einen Domänennamen registrieren, beachten Sie Folgendes:

- Sie können nur dann andere Zeichen als a-z, 0-9 und - (Bindestrich) verwenden, wenn die Top-Level-Domain (TLD) die Sprache, die Sie verwenden möchten, unterstützt und unterstützt IDNs . Informationen zur Ermittlung der von TLD unterstützten Sprachen finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.
- Sie können einen Namen in einer nicht unterstützten Sprache angeben, wenn der Name nur die Buchstaben a-z enthält. Wenn eine TLD beispielsweise kein Französisch unterstützt, der Name, den Sie verwenden möchten, jedoch nur die Zeichen a-z ohne diakritische Zeichen enthält, können Sie diesen Namen weiterhin verwenden. In diesem Beispiel ist ein Name mit einem „c“ zulässig; ein Name, der ein „ enthält, ist unzulässig.
- Wenn eine TLD die Sprache, die Sie für Ihren Domainnamen verwenden möchten, nicht unterstützt IDNs oder nicht unterstützt, können Sie den Namen auch nicht in Punycode angeben, obwohl der Punycode nur a-z, 0-9 und - enthält.

Das folgende Beispiel zeigt die Punycode-Darstellung des internationalisierten Domänennamens 中国.asia:

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

Wenn Sie einen IDN in die Adressleiste eines modernen Browsers eingeben, wandelt der Browser ihn vor der Übermittlung einer DNS-Abfrage oder HTTP-Anforderung in Punycode um.

Wie Sie einen IDN eingeben, hängt davon ab, was Sie erstellen möchten (Domänennamen, gehostete Zonen oder Datensätze) und wie Sie diese Objekte erstellen (über die API, das SDK oder die Route 53-Konsole):

- Wenn Sie die Route 53-API oder eine der APIs verwenden AWS SDKs, können Sie einen Unicode-Wert programmgesteuert in Punycode konvertieren. Wenn Sie z. B. mit Java arbeiten, können Sie einen Unicode-Wert in Punycode umwandeln, indem Sie die Methode toASCII der java.net.IDN-Bibliothek verwenden.
- Wenn Sie die Route 53-Konsole verwenden, um einen Domänennamen zu registrieren, können Sie den Namen (einschließlich Unicode-Zeichen) in das Namensfeld einfügen und die Konsole konvertiert den Wert vor dem Speichern in Punycode.
- Wenn Sie die Route 53-Konsole verwenden, um gehostete Zonen oder Datensätze zu erstellen, müssen Sie den Domänennamen in Punycode konvertieren, bevor Sie den Namen im entsprechenden Feld Name eingeben. Informationen zu Onlinekonvertern erhalten Sie, indem Sie eine Internetsuche nach „punycode converter“ durchführen.

Wenn Sie einen Domainnamen registrieren, beachten Sie, dass nicht alle Top-Level-Domains () dies unterstützen. TLDs IDNs Eine Liste der von Route 53 TLDs unterstützten Programme finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können. TLDs die nicht unterstützen, IDNs sind vermerkt.

Registrieren und Verwalten von Domainnamen unter Verwendung von Amazon Route 53

Wenn Sie einen neuen Domainnamen wie example.com als Teil der URL http://example.com möchten, können Sie ihn mit Amazon Route 53 registrieren. Sie können auch die Registrierung für vorhandene Domains von anderen Vergabestellen in Route 53 übertragen oder die Registrierung für Domains, die Sie mit Route 53 registriert haben, zu einer anderen Vergabestelle übertragen.

Die Verfahren in diesem Abschnitt erläutern, wie Sie mithilfe der Route-53-Konsole Domains registrieren und übertragen und wie Sie Domaineinstellungen bearbeiten und den Domainstatus anzeigen. Wenn Sie nur einige Domains registrieren und verwalten möchten, ist die Konsole die einfachste Möglichkeit.

Wenn Sie viele Domains registrieren und verwalten müssen, können Sie die Änderungen programmgesteuert vornehmen. Weitere Informationen finden Sie unter Amazon Route 53 einrichten.

> **Note**
>
> Wenn Sie eine Sprache verwenden, für die es ein AWS SDK gibt, verwenden Sie das SDK, anstatt zu versuchen, sich durch das zu arbeiten APIs. SDKs Sie vereinfachen die Authentifizierung, lassen sich problemlos in Ihre Entwicklungsumgebung integrieren und bieten einfachen Zugriff auf Route 53-Befehle.

Domainnamen-Registrierungsservices werden gemäß der Domainnamen-Registrierungsvereinbarung bereitgestellt.

Themen

- Konfigurieren von DNSSEC für eine Domäne
- Ihre Vergabestelle und andere Informationen zu Ihrer Domain finden
- Löschen einer Domainnamen-Registrierung
- Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support
- Herunterladen von Domains-Rechnungsberichten
- Domains, die Sie mit Amazon Route 53 registrieren können

Registrieren neuer Domains

Dieser Abschnitt behandelt die folgenden Themen im Zusammenhang mit der Registrierung neuer Domains bei Amazon Route 53:

1. Registrieren einer neuen Domain:
   - Erfahren Sie step-by-step, wie Sie mit der Route 53-Konsole eine neue Domain registrieren.
   - Machen Sie sich mit den Überlegungen und Voraussetzungen für die Domainregistrierung vertraut, wie z. B. die Kontaktaufnahme mit dem AWS Support bei Problemen, Preisen, unterstützten Top-Level-Domains (TLDs) und der automatischen Erstellung von Hosting-Zonen.
2. Angegebene Werte beim Registrieren oder Übertragen einer Domain:
   - Erfahren Sie, welche Werte Sie bei der Registrierung oder Übertragung einer Domain angeben müssen, einschließlich Kontaktinformationen, Datenschutzeinstellungen und Optionen für die automatische Verlängerung.
   - Machen Sie sich mit den Auswirkungen der Änderung bestimmter Werte vertraut, z. B. der E-Mail-Adresse des Domaininhabers oder Registranten.
3. Von Amazon Route 53 zurückgegebene Werte beim Registrieren einer Domain:
   - Erfahren Sie mehr über die Werte, die Route 53 nach erfolgreicher Domainregistrierung zurückgibt, einschließlich Registrierungsdatum, Ablaufdatum, Domain-Statuscodes, Übertragungssperrstatus und Nameserver.
4. Anzeigen des Status einer Domainregistrierung:
   - Erfahren Sie, wie Sie den aktuellen Status Ihrer Domainregistrierung einsehen können, einschließlich der ICANN-Statuscodes und aller Maßnahmen, die von Ihrer Seite aus erforderlich sind, wie z. B. die Überprüfung der E-Mail-Adresse des Registranten.

Registrieren einer neuen Domain

Registrieren einer neuen Domain oder Aktualisieren von Namenservern für eine bereits vorhandene Domain

Sie können Amazon Route 53 mit Domains verwenden, die Sie bei Route 53 registrieren und mit Domains, die Sie bei anderen DNS-Anbietern registriert haben. Wählen Sie je nach DNS-Anbieter eines der folgenden Verfahren aus, um eine neue Domain mit Route 53 zu registrieren und zu verwenden:

- Zum Registrieren einer neuen Domäne siehe So registrieren Sie eine neue Domäne mit Route 53.
- Informationen zu einer vorhandenen Domain finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.
- Informationen zum Verschieben einer Domain in eine andere Vergabestelle finden Sie unter Aktualisieren von Namenservern für die Verwendung eines anderen DNS-Service.

Überlegungen zur Domainregistrierung

Bevor Sie beginnen, beachten Sie Folgendes:

AWS Support kontaktieren

Wenn Sie bei der Registrierung einer Domain auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Preise für Domainregistrierung

Informationen zu den Kosten für die Registrierung von Domains finden Sie unter Amazon-Route-53-Preise für Domainregistrierung.

Unterstützte Domains

Eine Liste der unterstützten TLDs Programme finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können.

Sie können den Namen einer Domain nicht mehr ändern, nachdem Sie ihn registriert haben.

Wenn Sie versehentlich einen falschen Domainnamen registrieren, können Sie diesen nicht mehr ändern. Stattdessen müssen Sie einen weiteren Domainnamen registrieren und dabei

den richtigen Namen angeben. Sie können außerdem für einen versehentlich registrierten Domainnamen keine Erstattung erhalten.

AWS Credits

Sie können AWS Credits nicht verwenden, um die Gebühr für die Registrierung einer neuen Domain bei Route 53 zu bezahlen.

Spezial- oder Premium-Preise

Bei TLD Registrierungen sind einigen Domainnamen spezielle oder Premium-Preise zugeordnet. Für die Registrierung einer Domain mit einem Spezial- oder Premium-Preis kann Route 53 nicht verwendet werden.

Gebühren für gehostete Zonen

Wenn Sie mit Route 53 eine Domain registrieren, wird automatisch eine gehostete Zone für die Domain erstellt, für die eine kleine monatliche Gebühr zusätzlich zu der Jahresgebühr für die Domainregistrierung anfällt. In dieser gehosteten Zone speichern Sie Informationen darüber, wie Sie den Traffic für Ihre Domain weiterleiten, z. B. an eine EC2 Amazon-Instance oder eine CloudFront Distribution. Wenn Sie Ihre Domain noch nicht verwenden möchten, können Sie die gehostete Zone löschen. Wenn Sie diese innerhalb von 12 Stunden nach der Registrierung der Domain löschen, werden keine Gebühren für die gehostete Zone auf Ihrer AWS -Rechnung ausgewiesen. Wir erheben außerdem eine geringe Gebühr für die DNS-Abfragen, die wir für Ihre Domain erhalten. Weitere Informationen dazu finden Sie unter Amazon Route 53 – Preise.

Ersetzen der gehosteten Zone für eine Domain

Wenn Sie eine neue gehostete Zone für eine Domain erstellen, müssen Sie auch die Namenserver für die Domain aktualisieren, damit sie die gleichen Namenserver verwendet wie die neue gehostete Zone. Details hierzu finden Sie unter Ersetzen der gehosteten Zone für eine Domain, die bei Route 53 registriert ist.

So registrieren Sie eine neue Domäne mit Route 53

So registrieren Sie eine neue Domain mit Route 53

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich die Option Domains und anschließend Registrierte Domains aus.

3. Wählen Sie auf der Seite Registrierte Domains die Option Domains registrieren aus.

   a. Geben Sie im Abschnitt Nach Domain suchen den Domainnamen ein, den Sie registrieren möchten, und wählen Sie Suchen aus, um herauszufinden, ob der Domainname verfügbar ist.

      Wenn der Domainname, den Sie registrieren möchten, andere Zeichen als a-z, A-Z, 0-9 und - (Bindestrich) enthält, beachten Sie Folgendes:

      - Sie können den Namen mit den entsprechenden Zeichen eingeben. Sie müssen den Namen nicht in Punycode umwandeln.
      - Es wird eine Liste der Sprachen angezeigt. Wählen Sie die Sprache des angegebenen Namens. Wenn Sie beispielsweise příklad („Beispiel“ auf Tschechisch) eingeben, wählen Sie Tschechisch (CES) oder Tschechisch (CZE) aus.

        > **Note**
        >
        > Für Sprachen mit mehr als einem Code müssen Sie möglicherweise beide ausprobieren. Obwohl CES und CZE gleichbedeutend sind, unterstützen einige TLD-Register nur CES oder CZE.

      Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

      Wenn die von Ihnen eingegebene Domain verfügbar ist, wird sie angezeigt. Andernfalls werden ähnliche Domains als Vorschläge angezeigt.

      Sie können bis zu fünf Domains für die Registrierung auswählen. Die von Ihnen ausgewählten Domains werden in der Liste Ausgewählte Domains angezeigt.

   b. Wenn Sie mehrere Domains registrieren möchten, wiederholen Sie die Schritte 3a bis 3b.

4. Wählen Sie Zur Kasse gehen aus.

5. Wählen Sie auf der Seite Preise aus, für wie viele Jahre Sie die Domain registrieren möchten und ob Ihre Domainregistrierung vor dem Ablaufdatum automatisch verlängert werden soll.

> **Note**
>
> Registrierungen und Verlängerungen von Domainnamen sind nicht erstattungsfähig. Wenn Sie die automatische Domainverlängerung aktivieren und entscheiden, dass Sie den Domainnamen nach der Verlängerung der Registrierung nicht mehr wünschen, können Sie die Kosten der Verlängerung nicht erstattet bekommen.

Wählen Sie Weiter aus.

6. Geben Sie auf der Seite mit den Kontaktinformationen die Kontaktinformationen für den Domain-Registranten, den Administrator, die Techniker und die Rechnungsstellung ein. Die Werte, die Sie hier eingeben, gelten für alle Domains, die Sie registrieren. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain.

> **Important**
>
> Der Kontakt, den Sie bei der Domainregistrierung als Registrant angeben, hat gemäß der ICANN-Transferrichtlinie bestimmte Rechte als registrierter Namensinhaber des Domainnamens. Die meisten Domains werden nach der Schließung Ihrer Domain gelöscht AWS-Konto (weitere Informationen finden Sie unterMein AWS Konto ist geschlossen oder dauerhaft geschlossen und meine Domain ist bei Route 53 registriert). Bleibt eine Domain jedoch weiterhin in einem geschlossenen Konto, kann der Kontakt, den Sie als Registrant angegeben haben, möglicherweise die Übertragung des Domainnamens an einen externen Registrar beantragen. Daher ist es wichtig, dass der von Ihnen aufgeführte Registranten-Kontakt entweder Sie selbst oder eine andere Person ist, der Sie im Hinblick auf verantwortungsbewusstes Handeln vertrauen.

Beachten Sie die folgenden Überlegungen:

Vorname und Nachname

Wir empfehlen für First Name und Last Name den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen an den Domaineinstellungen erfordern manche Domainregistrierungen einen Identitätsnachweis. Der Name in Ihrer ID muss genau mit dem Namen des aktuellen Registrierenden der Domain übereinstimmen.

Unterschiedliche Kontakte

Standardmäßig verwenden wir die gleichen Informationen für alle drei Kontakte. Wenn Sie für einen oder mehrere der Kontakte andere Informationen eingeben möchten, deaktivieren Sie die Option Wie Registranten-Kontakt.

> **Note**
>
> Für .it-Domains müssen die registrierende Person und der administrative Kontakt identisch sein.

> **Note**
>
> Für .jp-Domains müssen die technischen und administrativen Ansprechpartner identisch sein.

Mehrere Domains

Wenn Sie mehr als eine Domain registrieren, verwenden wir die gleichen Kontaktinformationen für alle Domains.

Weitere erforderliche Informationen

Für einige Top-Level-Domains (TLDs) müssen wir zusätzliche Informationen sammeln. Geben Sie für diese TLDs Felder die entsprechenden Werte nach dem Feld PLZ/PLZ ein.

Datenschutz

Wählen Sie, ob Sie Ihre Kontaktinformationen vor WHOIS-Abfragen verbergen möchten.

> **Note**
>
> Sie müssen dieselbe Datenschutzeinstellung für die Ansprechpartner in den Bereichen Verwaltung, Registrant, Technik und Rechnungsstellung angeben.

Weitere Informationen finden Sie unter den folgenden Themen:

- Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne

- Domains, die Sie mit Amazon Route 53 registrieren können

> **Note**
>
> Zur Aktivierung des Datenschutzes für Domains vom Typ „.uk“, „co.uk“, „.me.uk“ und „.org.uk“ müssen Sie einen Support-Fall erstellen und Datenschutz anfordern.

Wählen Sie Weiter aus.

7. Überprüfen Sie auf der Seite Prüfen Ihre Angaben (und korrigieren Sie sie gegebenenfalls), lesen Sie die Servicevertragsbedingungen und aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bedingungen gelesen haben.

   Wählen Sie Absenden aus.

8. Wählen Sie im Navigationsbereich die Option Domains und anschließend Anforderungen aus.

   Auf dieser Seite können Sie sich den Status der Domain ansehen und auch ermitteln, ob Sie auf die Verifizierungs-E-Mail des Registranten-Kontakts antworten müssen. Außerdem können Sie die Verifizierungs-E-Mail erneut senden.

   Wenn Sie eine E-Mail-Adresse für den Registranten-Kontakt angegeben haben, die noch nie zur Registrierung einer Domain bei Route 53 verwendet wurde, müssen Sie bei einigen TLD-Registrierungsstellen die Gültigkeit der Adresse bestätigen.

   Anschließend wird eine Verifizierungs-E-Mail von einer der folgenden E-Mail-Adressen gesendet:

   - noreply@registrar.amazon — für die TLDs Registrierung bei Amazon Registrar.
   - noreply@domainnameverification.net oder noreply@emailverification.info — für die TLDs Registrierung durch unseren Registrar-Mitarbeiter Gandi. Die zuständige Vergabestelle für Ihre TLD finden Sie unter Wie Sie Ihre Vergabestelle finden.

> **Important**
>
> Der registrierende Kontakt muss die Anweisungen in der E-Mail befolgen, um zu bestätigen, dass die E-Mail-Adresse empfangen wurde. Andernfalls muss die Domain gesperrt werden, wie von ICANN gefordert. Wenn eine Domain gesperrt ist, kann im Internet nicht darauf zugegriffen werden.

a. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link in der E-Mail, um zu bestätigen, dass die E-Mail-Adresse gültig ist. Wenn Sie die E-Mail nicht sofort erhalten, überprüfen Sie Ihren Spam-Ordner.

b. Kehren Sie zur Seite Anforderungen zurück. Falls der Status nicht automatisch zu E-Mail-Adresse verifiziert aktualisiert wird, aktualisieren Sie den Browser.

9. Wenn die Domainregistrierung abgeschlossen ist, hängt der nächste Schritt davon ab, ob Sie Route 53 oder einen anderen DNS-Service als DNS-Service für die Domain verwenden möchten:

   - Route 53 – In der gehosteten Zone, die Route 53 bei der Registrierung der Domain erstellt hat, erstellen Sie Datensätze und teilen Route 53 mit, wie der Datenverkehr für die Domain und Subdomains weitergeleitet werden soll.

     Wenn zum Beispiel jemand den Domainnamen in einen Browser eingibt und diese Abfrage an Route 53 weitergeleitet wird, möchten Sie, dass Route 53 die Abfrage mit der IP-Adresse eines Webservers in Ihrem Rechenzentrum oder mit dem Namen eines ELB Load Balancers beantwortet?

     Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

     > **Important**
     >
     > Wenn Sie Datensätze in einer anderen gehosteten Zone erstellen als der, die Route 53 automatisch erstellt hat, müssen Sie die Nameserver für die Domain aktualisieren, sodass diese die Nameserver für die neue gehostete Zone verwenden.

   - Ein anderer DNS-Service – Konfigurieren Sie Ihre neue Domain zum Weiterleiten von DNS-Abfragen an den anderen DNS-Service. Führen Sie das Verfahren unter Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelle aus.

Angegebene Werte beim Registrieren oder Übertragen einer Domain

> **Note**
>
> Wir haben die Domainkonsole für Route 53 aktualisiert. Während der Übergangsphase können Sie die alte Konsole weiterverwenden oder die neue Konsole nutzen. Die meisten

von Route 53 zurückgegebenen Informationen sind für beide Konsolen identisch. Die Unterschiede sind in der folgenden Liste angegeben.

Wenn Sie eine Domain registrieren oder die Domainregistrierung an Amazon Route 53 übertragen, geben Sie die in diesem Thema beschriebenen Werte ein.

> **Note**
>
> Wenn Sie mehr als eine Domain registrieren, verwendet Route 53 die von Ihnen angegebenen Werte für alle Domains, die sich in Ihrem Warenkorb befinden.

Sie können auch Werte für eine Domain ändern, die derzeit in Route 53 registriert ist. Beachten Sie Folgendes:

- Wenn Sie die Kontaktinformationen für eine Domain ändern, senden wir eine E-Mail-Benachrichtigung über die Änderung an den Registrierenden. Diese E-Mail stammt von noreply@registrar.amazon. Für die meisten Änderungen ist es nicht erforderlich, dass der Registrierende antwortet.
- Für Änderungen an Kontaktinformationen, die auch eine Änderung des Eigentümers bedeuten, senden wir dem Registranten-Kontakt eine zusätzliche E-Mail. ICANN verlangt, dass der Registranten-Kontakt den E-Mail-Empfang bestätigt. Weitere Informationen finden Sie unter Vorname, Nachname und Organisation weiter unten in diesem Abschnitt.

Weitere Informationen zum Ändern von Einstellungen für eine vorhandene Domain finden Sie unter Aktualisieren von Domaineinstellungen .

Werte, die Sie angeben

- 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

Identisch mit der Kontaktperson des Registranten

Gibt an, ob die gleichen Kontaktinformationen für den Registrierenden der Domains, den administrativen und den technischen Kontakt verwendet werden sollen.

Kontakttyp

Kategorie für diesen Kontakt. Beachten Sie Folgendes:

- Wenn Sie eine andere Option als Person wählen, müssen Sie einen Organisationsnamen eingeben.
- In einigen TLDs Fällen hängt der verfügbare Datenschutz von dem Wert ab, den Sie für Kontakttyp wählen. Informationen zu den Datenschutzeinstellungen für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.
- Für .es-Domains muss der Wert von Contact Type (Kontakttyp) bei allen drei Kontakten Person lauten.

Vorname, Nachname

Vor- und Nachname des Kontakts.

> **Important**
>
> Wir empfehlen für First Name und Last Name den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen der Domaineinstellungen müssen Sie sich ausweisen und der Name auf Ihrem Ausweis muss mit dem Namen des Registrierenden der Domain übereinstimmen.

Wenn Sie eine Domain an Route 53 übertragen und die folgenden Bedingungen erfüllt sind, ändern Sie den Eigentümer der Domain:

- Der Kontakttyp lautet Person.
- Sie ändern die Felder Vorname and/or Nachname für den Kontakt mit dem Registranten gegenüber den aktuellen Einstellungen.

In diesem Fall verlangt ICANN, dass der Registranten-Kontakt zur Bestätigung per E-Mail kontaktiert wird. Wir senden eine E-Mail von einer der folgenden E-Mail-Adressen:

TLDs	E-Mail-Adresse, von der die Bestätigungs-E-Mail kommt
TLDs registriert von Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (Die E-Mail wird sowohl an den aktuellen Registrierenden als auch an den neuen Registrierenden gesendet.)
Alle anderen	noreply@domainnameverification.net oder noreply@emailverification.info

Die zuständige Vergabestelle für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

> **Important**
>
> Der Registrierende muss die Anweisungen in der E-Mail befolgen, um zu bestätigen, dass die E-Mail-Adresse empfangen wurde, andernfalls müssen wir die Domain sperren, wie von ICANN gefordert. Wenn eine Domain gesperrt ist, kann im Internet nicht darauf zugegriffen werden.

Wenn Sie die E-Mail-Adresse für den Registrierenden ändern, senden wir diese E-Mail an die bisherige und die neue E-Mail-Adresse für den Registrierenden.

Einige TLD-Vergabestellen berechnen eine Gebühr für das Ändern des Domaineigentümers. Wenn Sie einen dieser Werte verändern, zeigt die Route-53-Konsole eine Meldung an, in der Sie darüber informiert werden, ob eine Gebühr anfällt.

Organisation

Die Organisation, die dem Kontakt zugeordnet ist (falls zutreffend). Für den Registrierenden und administrative Kontakte ist dies in der Regel die Organisation, welche die Domain registriert. Für den technischen Kontakt kann dies die Organisation sein, welche die Domain verwaltet.

Wenn der Kontakttyp ein anderer Wert als Person ist und Sie das Feld Organization für den Registrierenden ändern, ändern Sie damit den Eigentümer der Domain. ICANN verlangt, dass der Registrierende zur Bestätigung per E-Mail kontaktiert wird. Wir senden eine E-Mail von einer der folgenden E-Mail-Adressen:

TLDs	E-Mail-Adresse, von der die Bestätigungs-E-Mail kommt
TLDs registriert von Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (Die E-Mail wird sowohl an den aktuellen Registrierenden als auch an den neuen Registrierenden gesendet.)
Alle anderen	noreply@domainnameverification.nett oder noreply@emailverification.info

Die zuständige Vergabestelle für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

Wenn Sie die E-Mail-Adresse für den Registrierenden ändern, senden wir diese E-Mail an die bisherige und die neue E-Mail-Adresse für den Registrierenden.

Einige TLD-Vergabestellen berechnen eine Gebühr für das Ändern des Domaineigentümers. Wenn Sie den Wert für Organization (Organisation) verändern, zeigt die Route-53-Konsole eine Meldung an, in der Sie darüber informiert werden, ob eine Gebühr anfällt.

E-Mail

Die E-Mail-Adresse des Kontakts.

Wenn Sie die E-Mail-Adresse für den Registrierenden ändern, senden wir eine Benachrichtigungs-E-Mail an die bisherige und die neue E-Mail-Adresse. Diese E-Mail stammt von noreply@registrar.amazon.

Telefon

Die Telefonnummer des Kontakts:

- Wenn Sie eine Rufnummer für Standorte in den USA und Kanada eingeben, geben Sie 1 im ersten Feld und die 10-stellige Vorwahl und Telefonnummer im zweiten Feld ein.
- Wenn Sie eine Rufnummer für einen anderen Standort eingeben, geben Sie den Ländercode im ersten Feld und den Rest der Telefonnummer im zweiten Feld ein. Eine Liste der Telefon-Ländercodes finden Sie im Wikipedia-Artikel Liste der internationalen Vorwahlnummern.

Adresse 1

Die Straße der Adresse des Kontakts.

Adresse 2

Zusätzliche Adressinformationen des Kontakts, z. B. Wohnungsnummer oder Postfach.

Land

Das Land des Kontakts.

Status

Das Bundesland des Kontakts, sofern vorhanden.

Ort

Der Wohnort des Kontakts.

Postleitzahl

Die Postleitzahl des Kontakts.

Felder für ausgewählte Top-Level-Domains

Für die folgenden Top-Level-Domains (TLDs) müssen Sie zusätzliche Werte angeben:

- .com.au und .net.au
- .ca
- .es
- .fi
- .fr

- .it
- .ru
- .se
- .sg
- „.co.uk“, „.me.uk“, „.org.uk“ und „.uk“

Darüber hinaus TLDs benötigen viele eine Umsatzsteuer-Identifikationsnummer.

Informationen zu gültigen Werten finden Sie ExtraParamin der Amazon Route 53 API-Referenz.

Datenschutz

Wählen Sie, ob Sie Ihre Kontaktinformationen vor WHOIS-Abfragen verbergen möchten. Wenn Sie Datenschutz aktivieren (neue Konsole) oder Kontaktinformationen ausblenden (alte Konsole) auswählen, geben WHOIS-Abfragen („Wer ist wer?“) Kontaktinformationen für die Vergabestelle oder den Wert „Durch Richtlinie geschützt“ zurück.

> **Note**
>
> Sie müssen dieselbe Datenschutzeinstellung für die Ansprechpartner in den Bereichen Verwaltung, Registrant, Technik und Rechnungsstellung angeben.

Wenn Sie Kontaktinformationen nicht ausblenden auswählen, erhalten Sie unter der E-Mail-Adresse, die Sie angegeben haben, mehr E-Mail-Spam.

Jeder kann eine WHOIS-Abfrage für eine Domain senden und erhält alle Kontaktinformationen für diese Domain. Der WHOIS-Befehl ist in vielen Betriebssystemen verfügbar und steht zudem als Webanwendung auf vielen Webseiten zur Verfügung.

> **Important**
>
> Obwohl es berechtigte Benutzer für die Kontaktinformationen Ihrer Domain gibt, sind es meist Spammer, die unerwünschte E-Mail- und Spam-Angebote an Domainkontakte senden. Grundsätzlich empfehlen wir, dass Sie Kontaktinformationen ausblenden (Option Privacy Protection).

Zur Aktivierung oder Deaktivierung des Datenschutzes für einige Domains müssen Sie einen Support-Fall eröffnen und Datenschutz anfordern.

Weitere Informationen zum Datenschutz finden Sie in den folgenden Themen:

- Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne
- Domains, die Sie mit Amazon Route 53 registrieren können

Automatische Verlängerung (nur verfügbar, wenn Sie die Domaineinstellungen bearbeiten)

Legen Sie fest, ob Route 53 die Domain vor dem Ablauf automatisch verlängern soll. Die Anmeldegebühr wird Ihrem AWS Konto belastet. In der alten Konsole ist diese Einstellung nur beim Bearbeiten von Domaineinstellungen verfügbar. Weitere Informationen finden Sie unter Verlängern der Registrierung für eine Domain.

> **Important**
>
> Wenn Sie die automatische Verlängerung deaktivieren, wird die Registrierung für die Domain nicht erneuert, wenn das Ablaufdatum vorbei ist. Deshalb ist es möglich, dass Sie den Domainnamen verlieren.

Der Zeitraum, in dem Sie einen Domainnamen erneuern können, variiert je nach Top-Level-Domain (TLD). Eine Übersicht über die Domainverlängerung finden Sie unter Verlängern der Registrierung für eine Domain. Weitere Informationen zum Verlängern der Domainregistrierung für eine bestimmte Anzahl von Jahren finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

Von Amazon Route 53 zurückgegebene Werte beim Registrieren einer Domain

Wenn Sie Ihre Domain bei Amazon Route 53 registrieren, gibt Route 53 die folgenden Werte zusätzlich zu den Werten zurück, die Sie angegeben haben.

Registriert am

Das Datum, an dem die Domain ursprünglich mit Route 53 registriert wurde.

Gültig bis

Das Datum und die Uhrzeit, wann der aktuelle Registrierungszeitraum endet, in Greenwich Mean Time (GMT).

Die Registrierungsfrist beträgt in der Regel ein Jahr, obwohl die Registries für einige Top-Level-Domains (TLDs) längere Registrierungszeiträume haben. Informationen zum Registrierungs- und Verlängerungszeitraum für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

In den meisten TLDs Fällen können Sie den Registrierungszeitraum um bis zu zehn Jahre verlängern. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

Domainnamen-Statuscode

Der aktuelle Status der Domain.

ICANN, die Organisation, die eine zentrale Datenbank mit Domainnamen verwaltet, hat eine Reihe von Statuscodes für Domainnamen (auch als EPP-Statuscodes bezeichnet) entwickelt, die Aufschluss über den Status verschiedener Vorgänge für einen Domainnamen geben. Hierzu zählen beispielsweise die Registrierung eines Domainnamens, die Übertragung eines Domainnamens an eine andere Vergabestelle und die Verlängerung der Registrierung für einen Domainnamen. Alle Vergabestellen verwenden dieselben Statuscodes.

Eine aktuelle Liste der Domainnamen-Statuscodes und eine Erläuterung, was jeder Code bedeutet, finden Sie auf der ICANN-Website unter dem Stichwort EPP Statuscodes. (Suchen Sie auf der ICANN-Website, Web-Suchvorgänge geben gelegentlich eine veraltete Version des Dokuments zurück.)

Übertragungssperre

Gibt an, ob die Domain gesperrt ist, um das Risiko zu reduzieren, dass jemand ohne Ihre Zustimmung Ihre Domain an eine andere Vergabestelle überträgt. Wenn die Domain gesperrt ist, hat Transfersperre den Wert Ein. Wenn die Domain nicht gesperrt ist, lautet der Wert Aus.

Automatische Verlängerung

Gibt an, ob Route 53 automatisch die Registrierung für diese Domain kurz vor dem Ablaufdatum verlängert.

Autorisierungscode

Der Code, der erforderlich ist, wenn Sie die Registrierung dieser Domain an eine andere Vergabestelle übertragen möchten. Ein Autorisierungscode wird nur generiert, wenn Sie es angefordert haben. Informationen zum Übertragen einer Domain an eine andere Vergabestelle finden Sie unter Überträgt eine Domain von Amazon Route 53 zu einer anderen Vergabestelle..

Nameserver

Die Route-53-Server, die auf DNS-Abfragen für diese Domain antworten. Wir empfehlen, dass Sie die Route-53-Namensserver nicht löschen.

Weitere Informationen zum Hinzufügen, Ändern oder Löschen von Namensservern finden Sie unter Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Anzeigen des Status einer Domainregistrierung

ICANN, die Organisation, die eine zentrale Datenbank mit Domainnamen verwaltet, hat eine Reihe von Statuscodes für Domainnamen (auch als EPP-Statuscodes bezeichnet) entwickelt, die Ihnen den Status für eine Vielzahl von Vorgängen anzeigen, zum Beispiel einen Domainnamen registrieren, einen Domainnamen an eine andere Vergabestelle übertragen, Registrierung für einen Domainnamen verlängern und so weiter. Alle Vergabestellen verwenden dieselben Statuscodes.

Um den Statuscode Ihrer Domains anzuzeigen, führen Sie die folgenden Schritte aus.

So zeigen Sie den ICANN-Statuscode einer Domain an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie im Navigationsbereich die Option Domains und wählen Sie Registrierte Domains aus.
3. Wählen Sie den verknüpften Namen Ihrer Domain aus.
4. Falls eine Aktion Ihrerseits erforderlich ist (z. B. das erneute Senden der Verifizierungs-E-Mail an den Registranten-Kontakt), gibt ein Banner am oberen Seitenrand Aufschluss über die auszuführende Aktion.
5. Der aktuelle Status Ihrer Domain wird durch den Wert im Feld Domainstatuscode angegeben.

   Eine aktuelle Liste der Domainnamen-Statuscodes und eine Erläuterung, was jeder Code bedeutet, finden Sie auf der ICANN-Website unter dem Stichwort EPP Statuscodes. (Suchen Sie auf der ICANN-Website, Web-Suchvorgänge geben gelegentlich eine veraltete Version des Dokuments zurück.)

Der Status der Registrierung ist auch auf der Seite Anforderungen verfügbar.

So zeigen Sie den Registrierungsstatus an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie im Navigationsbereich die Option Domains und wählen Sie Anforderungen aus.
3. Auf der Seite Anforderungen können Sie sich sowohl den Registrierungsstatus als auch den Status anderer Aktionen ansehen, die Sie für Domains ausgeführt haben. Beispiele wären etwa das Löschen von Domains, das Sperren von Domainübertragungen sowie das Hinzufügen oder Löschen von DNSSEC-Schlüsseln.

   Außerdem werden Aktionen aufgeführt, die ggf. zum Abschließen eines Prozesses ausgeführt werden müssen (beispielsweise die Bestätigung Ihrer E-Mail-Adresse).

   - Um auf eine Aktionsanforderung zu reagieren, wählen Sie das Optionsfeld neben dem Domainnamen und anschließend in der Dropdownliste Aktion die Aktion aus.

Aktualisieren von Domaineinstellungen

Dieser Abschnitt enthält Informationen zu den folgenden Themen im Zusammenhang mit der Verwaltung von Domäneneinstellungen in Route 53:

1. Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne:
   - Erfahren Sie, wie Sie Kontaktinformationen für eine Domain aktualisieren, einschließlich administrativer, technischer, Registrant- und Rechnungskontakte.
   - Machen Sie sich mit dem Verfahren zum Ändern des Inhabers einer Domain vertraut, wenn die Registry ein Formular zur Änderung des Domaininhabers verlangt.
2. Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne:
   - Erfahren Sie, wie Sie den Datenschutz für Kontaktinformationen aktivieren oder deaktivieren können, der Ihre persönlichen Daten vor WHOIS-Abfragen verbirgt oder enthüllt.
3. Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne:
   - Erfahren Sie, wie Sie die automatische Verlängerung für eine Domain aktivieren oder deaktivieren, die bestimmt, ob Route 53 die Registrierung vor Ablauf automatisch erneuert.
4. Sperren einer Domäne zum Verhindern der nicht autorisierten Übertragung an eine andere Vergabestelle:

- Erfahren Sie, wie Sie eine Domain sperren, um eine unbefugte Übertragung an einen anderen Registrar zu verhindern, und wie Sie die Sperre bei Bedarf deaktivieren.

5. Verlängern des Registrierungszeitraums für eine Domäne:
   - Machen Sie sich mit dem Verfahren zur Verlängerung des Registrierungszeitraums für eine Domain vertraut, in der Regel auf bis zu zehn Jahre in Schritten von einem Jahr.
6. Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelleund: Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne
   - Erfahren Sie, wie Sie Nameserver aktualisieren, um einen anderen DNS-Dienst zu verwenden, oder White-Label-Nameserver (Vanity) konfigurieren.
   - Erfahren Sie mehr über Überlegungen und bewährte Methoden beim Ändern von Nameservern und Glue-Records.

Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne

Für die administrativen und technischen Kontakte für eine Domäne können Sie alle Kontaktinformationen ändern, ohne die Änderungen zu autorisieren. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen für eine Domäne.

Für den Registrierenden können Sie die meisten Werte ändern, ohne die Änderungen zu autorisieren. Für einige TLDs ist für den Wechsel des Inhabers einer Domain jedoch eine Autorisierung erforderlich. Weitere Informationen finden Sie im entsprechenden Thema.

Themen

- Was löst eine Änderung der Domaininhaberschaft aus?
- TLDs die eine besondere Bearbeitung erfordern, um den Besitzer zu wechseln
- Aktualisieren der Kontaktinformationen für eine Domäne
- Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert

Was löst eine Änderung der Domaininhaberschaft aus?

> **Important**
>
> Der Kontakt, den Sie als Registrant angeben, hat gemäß der ICANN-Übertragungsrichtlinie bestimmte Rechte als registrierter Inhaber des Domainnamens. Die meisten Domains werden

nach der Schließung Ihrer Domain gelöscht AWS-Konto (weitere Informationen finden Sie unterMein AWS Konto ist geschlossen oder dauerhaft geschlossen und meine Domain ist bei Route 53 registriert). Bleibt eine Domain jedoch weiterhin in einem geschlossenen Konto, kann die Kontaktperson, die Sie als Registrant angegeben haben, möglicherweise die Übertragung des Domainnamens an einen externen Registrar beantragen. Daher ist es wichtig, dass der von Ihnen aufgeführte Registranten-Kontakt entweder Sie selbst oder eine andere Person ist, der Sie im Hinblick auf verantwortungsbewusstes Handeln vertrauen.

Die folgenden Änderungen an den Kontaktinformationen des Registranten lösen den Prozess zur Änderung des Domaininhabers aus:

Geben Sie für Person den Kontakttyp ein

Das Ändern der Felder Vorname oder Nachname löst einen Eigentümerwechsel aus.

Für Kontakttypen, die keine Person sind (Unternehmen, Vereinigung, öffentliche Einrichtung)

Eine Änderung des Felds Organisation löst einen Eigentümerwechsel aus.

Zusätzliche Auslöser (alle Kontakttypen)

Abhängig von den TLD-Anforderungen Ihrer Domain können auch andere Änderungen des Kontaktfeldes den Prozess des Eigentümerwechsels auslösen, darunter:

- Änderungen an der E-Mail-Adresse des Registranten
- Änderungen an anderen Feldern mit identifizierenden Informationen

Die spezifischen Felder, die Eigentümerwechsel auslösen, variieren je nach TLD und werden durch die Richtlinien der Domain-Registry bestimmt.

Warning

Risiko einer Betriebsunterbrechung: Wenn ein Eigentümerwechsel ausgelöst wird, erhalten Sie eine Autorisierungs-E-Mail. Wenn Sie nicht innerhalb von 3-15 Tagen auf diese E-Mail antworten (abhängig von Ihrer TLD), wird Ihre Domainregistrierung gemäß den Vorgaben der ICANN storniert, wodurch Ihre Website und Ihre E-Mail-Dienste unterbrochen werden. Stellen Sie immer sicher, dass Sie auf die Kontakt-E-Mail-Adresse des Registranten zugreifen können, bevor Sie Kontaktänderungen vornehmen.

Beachten Sie Folgendes beim Ändern des Domäneneigentümers:

- Für einige TLDs ist der Wechsel des Inhabers einer Domain kostenpflichtig. Um zu bestimmen, ob für die TLD für Ihre Domain eine Gebühr erhoben wird, schauen Sie unter „Preis für Änderung des Eigentümers“ in der Spalte Amazon-Route-53-Preise für Domainregistrierung.

  > **Note**
  >
  > Sie können AWS Credits nicht verwenden, um die Gebühr zu zahlen, falls eine Gebühr anfällt, um den Besitzer einer Domain zu wechseln.

- In einigen TLDs Fällen senden wir, wenn Sie den Inhaber einer Domain ändern, eine Autorisierungs-E-Mail an die E-Mail-Adresse des Registranten. Der Registrierende muss Sie die Anweisungen in der E-Mail befolgen, um die Änderung zu autorisieren.
- Bei einigen TLDs müssen Sie ein Formular zur Änderung des Domainbesitzes ausfüllen und einen Identitätsnachweis vorlegen, damit ein Support-Techniker von Amazon Route 53 die Werte für Sie aktualisieren kann. Wenn die TLD für Ihre Domäne ein Formular zum Ändern des Domäneneigentümers erfordert, zeigt die Konsole eine Nachricht mit einem Link zu einem Formular an, das für Sie einen Support-Vorgang öffnet. Weitere Informationen finden Sie unter Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

TLDs die eine besondere Bearbeitung erfordern, um den Besitzer zu wechseln

Wenn Sie den Inhaber einer Domain ändern, TLDs erfordern die Registrierungen einiger Domains eine besondere Bearbeitung. Wenn Sie den Besitzer für eine der folgenden Domänen ändern, führen Sie das entsprechende Verfahren aus. Wenn Sie den Besitzer für eine andere Domäne ändern, können Sie den Besitzer selbst ändern, entweder programmgesteuert oder über die Route-53-Konsole. Siehe Aktualisieren der Kontaktinformationen für eine Domäne.

Folgendes TLDs erfordert eine spezielle Bearbeitung, um den Inhaber der Domain zu ändern:

.be, .cl, .com.br, .es, .fi, .ru, .se, .sh

.be

Sie müssen von der Registrierungsstelle einen Transfercode für.be-Domains erhalten und dann einen Fall beim AWS Support einreichen.

- Den Transfercode finden Sie unter https://www.dnsbelgium. be/en/manage-your-domain-name/change-holder #transfer, und folgen Sie den Anweisungen.
- Informationen zum Öffnen eines Kundenvorfalls finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

.cl

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.com.ar

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.com.br

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.es

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.fi

Starten Sie die Änderung des Besitzers auf der Route-53-Konsole. Nachdem Sie die Änderung veranlasst haben, erhalten Sie von der fi-domain-tech@traficom .fi-E-Mail-Adresse einen Holder-Transferschlüssel. Nachdem Sie den Schlüssel erhalten haben, öffnen Sie eine Support-Anfrage beim AWS Support und teilen Sie uns den Schlüsselcode mit. Siehe Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

.qa

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.ru

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.se

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

.sh

Sie müssen ein Formular ausfüllen und an den AWS Support senden. Siehe Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert.

Aktualisieren der Kontaktinformationen für eine Domäne

Um die Kontaktinformationen für eine Domäne zu aktualisieren, führen Sie folgende Schritte durch.

> **Warning**
>
> Risiko einer Betriebsunterbrechung: Wenn Ihre Kontaktänderung den Eigentümerwechsel auslöst, erhalten Sie eine Autorisierungs-E-Mail. Wenn Sie nicht innerhalb von 3-15 Tagen (abhängig von Ihrer TLD) auf diese E-Mail antworten, wird Ihre Domainregistrierung gemäß den Vorgaben der ICANN storniert, wodurch Ihre Website und Ihre E-Mail-Dienste unterbrochen werden.
> Stellen Sie sicher, dass Sie auf die Kontakt-E-Mail-Adresse des Registranten zugreifen können, bevor Sie Kontaktänderungen vornehmen.

Vor dem Aktualisieren der Domain-Kontakte

Bevor Sie Änderungen an den Kontaktinformationen des Registranten Ihrer Domain vornehmen, füllen Sie diese Checkliste aus:

1. ☐ E-Mail-Zugriff verifizieren — Bestätigen Sie, dass Sie E-Mails an die aktuelle E-Mail-Adresse des Registranten erhalten können

2. ☐ Verstehen Sie die Auslöser für den Eigentümerwechsel — Prüfen the section called “Was löst eine Änderung der Domaininhaberschaft aus?” Sie, welche Änderungen den Prozess des Eigentümerwechsels auslösen könnten
3. ☐ Plane mögliche Ausfallzeiten ein — Wenn ein Inhaberwechsel ausgelöst wird, hast du 3—15 Tage Zeit, um auf die Autorisierungs-E-Mail zu antworten, andernfalls wird deine Domain gekündigt

So aktualisieren Sie die Kontaktinformationen für eine Domäne

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie den Namen der Domäne aus, deren Kontaktinformationen Sie aktualisieren möchten.
4. Wählen Sie auf dem Tab Kontaktinformationen die Option Bearbeiten aus.
5. Wenn Sie keinen Zugriff auf die E-Mail-Adresse für den Kontakt mit dem Registranten haben, gehen Sie wie folgt vor. Wenn Sie Zugriff auf die E-Mail-Adresse des Kontakts für den Registranten haben, fahren Sie mit Schritt 6 fort.

   a. Ändern Sie nur die E-Mail-Adresse für den Registranten-Kontakt. Ändern Sie keine weiteren Werte für jegliche Kontakte der Domäne. Wenn Sie außerdem weitere Werte ändern möchten, tun Sie dies zu einem späteren Zeitpunkt.

      Wählen Sie Änderungen speichern aus.

      Wir senden eine Verifizierungs-E-Mail an die neue Adresse (falls dies für die TLD erforderlich ist), um die neue E-Mail-Adresse zu verifizieren. Sie müssen den Link in der E-Mail auswählen, um zu bestätigen, dass die neue E-Mail-Adresse gültig ist. Wenn eine Überprüfung erforderlich ist und Sie die neue E-Mail-Adresse nicht verifizieren, setzt Route 53 die Domain wie von ICANN erforderlich aus.

      Wenn Sie die Verifizierungs-E-Mail erneut senden müssen, navigieren Sie zur Seite Registrierte Domains, aktivieren Sie das Optionsfeld neben dem aktualisierten Domainnamen und wählen Sie den Namen der Domain aus, die Sie aktualisieren möchten. Wählen Sie in der Warnung Verifizieren Sie Ihre E-Mail, um eine Domainsperre zu vermeiden die Option E-Mail erneut senden aus.

b. Wenn Sie andere Werte für den Registranten, Administrator, Techniker oder Rechnungskontakt für die Domain ändern möchten, kehren Sie zu Schritt 1 zurück und wiederholen Sie den Vorgang.

6. Aktualisieren Sie die entsprechenden Werte. Sie können auch Registranten-Kontakt kopieren auswählen, um automatisch die gleichen Informationen auszufüllen, die Sie für den Registranten-Kontakt eingegeben haben. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain.

   Abhängig von der TLD für Ihre Domäne und die Werte, die Sie ändern, zeigt die Konsole ggf. die folgende Meldung an:

   "Um den Namen des Registrierenden oder die Organisation zu ändern, eröffnen Sie einen Fall."

   Wenn Sie diese Meldung sehen, können Sie den Rest dieses Vorgangs überspringen und erhalten in Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert weitere Informationen.

7. Wählen Sie Speichern.

8. Wenn Sie den Eigentümer einer Domäne ändern, wie unter Was löst eine Änderung der Domaininhaberschaft aus? beschrieben, senden wir eine E-Mail an den Registrierenden für die Domäne. Die E-Mail fragt nach der Autorisierung für die Änderung des Eigentümers.

   Wenn Sie nicht innerhalb von 3 bis 15 Tagen nach der Änderung die Autorisierung erhalten, abhängig von der Top-Level-Domain, müssen wir die Anforderung gemäß ICANN stornieren.

   Die E-Mail kommt von einer der folgenden E-Mail-Adressen.

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
Alle anderen	Eine der folgenden E-Mail-Adressen: •

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt
	noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

9. Wenn Sie beim Aktualisieren der Kontaktinformationen auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Informationen zur API, mit der Sie die Kontaktinformationen aktualisieren können, finden Sie unter UpdateDomainContact.

Ändern des Eigentümers einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert

Wenn die Registry für Ihre Domain verlangt, dass Sie einen Domaininhaberwechsel durchführen und das Formular an den AWS Support senden, gehen Sie wie folgt vor. Um festzustellen, ob Sie dieses Verfahren ausführen müssen, lesen Sie die folgenden Themen:

- Um zu bestimmen, ob die von Ihnen vorgenommene Änderung des Werts als Änderung des Eigentümers betrachtet wird, siehe Was löst eine Änderung der Domaininhaberschaft aus?.
- Informationen zum Bestimmen, ob für Ihre Domäne in ein Formular zur Änderung des Domänenbesitzes erforderlich ist, finden Sie unter TLDs die eine besondere Bearbeitung erfordern, um den Besitzer zu wechseln.

So ändern Sie den Eigentümer einer Domäne, wenn die Registrierung ein Formular zum Ändern des Domäneneigentümers erfordert

1. Informieren Sie sich in der Einführung zu diesem Thema, um zu bestimmen, ob die Registrierung für Ihre Domäne eine spezielle Verarbeitung zur Änderung des Eigentümers der Domäne erfordert. Ist dies der Fall und es wird ein Formular zum Ändern des Domäneneigentümers benötigt, setzen Sie den Vorgang wie folgt fort.

Wenn kein Formular zum Ändern des Domäneneigentümers erforderlich ist, führen Sie stattdessen die Schritte im entsprechenden Thema aus.

2. Laden Sie das Formular zum Ändern des Domäneneigentümers herunter. Die Datei wird in eine ZIP-Datei komprimiert.
3. Füllen Sie das Formular aus.
4. Holen Sie für den Registranten-Kontakt für den früheren Eigentümer der Domäne und für den neuen Eigentümer eine Kopie eines unterschriebenen Identitätsnachweises (Personalausweis, Führerschein, Pass oder einen anderen rechtsgültigen Identitätsnachweis) ein.

   Wenn eine juristische Person als registrierende Organisation aufgelistet ist, holen Sie außerdem die folgenden Informationen für den früheren Eigentümer der Domäne und für den neuen Eigentümer ein:

   - Nachweis, dass die Organisation, auf die die Domäne registriert ist, existiert.
   - Nachweis, dass die Vertreter für den früheren Eigentümer und den neuen Eigentümer autorisiert sind, im Namen der Organisation zu handeln. Dieses Dokument muss ein zertifiziertes rechtliche Dokument sein, das den Namen der Organisation und die Namen der Vertreter als Zeichnungsberechtigte (z. B. CEO, Direktor oder Geschäftsführer) enthält.
5. Scannen Sie das Formular zum Ändern des Domäneneigentümers und die erforderlichen Nachweise. Speichern Sie die gescannten Dokumente in einem allgemeinen Format, z. B. als PDF-Datei oder PNG-Datei.
6. Melden Sie sich mit dem AWS Konto, für das die Domain derzeit registriert ist, beim AWS Support Center an.

   Important

   Sie müssen sich entweder mit dem Stammkonto oder mit einem Benutzer anmelden, dem auf eine oder mehrere der folgenden Arten IAM-Berechtigungen gewährt wurden:

   - Dem Benutzer wird die AdministratorAccessverwaltete Richtlinie zugewiesen.
   - Dem Benutzer wird die DomainsFullAccess verwaltete Richtlinie AmazonRoute53 zugewiesen.
   - Dem Benutzer wird die FullAccess verwaltete Richtlinie AmazonRoute53 zugewiesen.

Wenn Sie sich weder mit dem Stammkonto noch mit einem Benutzer anmelden, der über die erforderlichen Berechtigungen verfügt, können wir den Domaineigentümer nicht aktualisieren. Diese Voraussetzung verhindert, dass nicht autorisierte Benutzer den Eigentümer einer Domäne ändern.

7. Geben Sie die folgenden Werte an:

   Regarding

   Akzeptieren Sie den Standardwert für Konto und Abrechnung.

   Service

   Akzeptieren Sie den Standardwert von Domains.

   Kategorie

   Akzeptieren Sie den Standardwert „Eigentümerwechsel“.

   Schweregrad

   Akzeptieren Sie den Standardwert „Allgemeine Frage“.

   Klicken Sie auf Next step (Nächster Schritt): Additional information (Zusätzliche Informationen)

   Betreff

   Geben Sie Change the owner of a domain an.

   Description

   Geben Sie die folgenden Informationen ein:

   - Domäne, deren Eigentümer Sie ändern möchten
   - 12-stellige Konto-ID des AWS Kontos, für das die Domain registriert ist

   Add attachment

   Laden Sie die Dokumente hoch, die Sie in Schritt 5 eingescannt haben.

   Kontaktmethode

   Geben Sie eine Kontaktmethode an, und geben Sie die entsprechenden Werte ein.

8. Wählen Sie Absenden aus.

Ein AWS Support-Techniker überprüft die von Ihnen bereitgestellten Informationen und aktualisiert die Einstellungen. Der Techniker wird sich mit Ihnen in Verbindung setzen, wenn die Aktualisierung beendet ist, oder um weitere Informationen bitten.

Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne

Wenn Sie eine Domain bei Amazon Route 53 registrieren oder eine Domain auf Route 53 übertragen, aktivieren wir standardmäßig den Datenschutz für alle Kontakte für die Domain. Dies blendet in der Regel die meisten Ihrer Kontaktinformationen aus WHOIS-Abfragen ("Wer ist wer?") aus und reduziert die Menge der Spam-Nachrichten, die Sie erhalten. Wenn Sie den Datenschutz aktivieren, werden Ihre Kontaktinformationen durch die Kontaktinformationen der Registrierungsstelle oder durch den Satz „REDACTED FOR PRIVACY“ (AUS DATENSCHUTZGRÜNDEN UNKENNTLICH GEMACHT) oder „On behalf of <domain name> owner“ (Im Namen von Eigentümer von <Domainname>) ersetzt.

Wenn Sie den Datenschutz deaktivieren möchten, müssen Sie ihn für alle Kontakte für eine Domäne deaktivieren. Wenn Sie den Datenschutz deaktivieren, kann jeder eine WHOIS-Anfrage für die Domain senden und kann bei den meisten Top-Level-Domains (TLDs) möglicherweise alle Kontaktinformationen abrufen, die Sie bei der Registrierung oder Übertragung der Domain angegeben haben, einschließlich Name, Adresse, Telefonnummer und E-Mail-Adresse. Der WHOIS-Befehl ist weithin verfügbar. Er ist in vielen Betriebssystemen enthalten und steht zudem als Webanwendung auf vielen Webseiten zur Verfügung.

Wenn Sie eine Domain an einen anderen Registrar übertragen und der Datenschutz für die Domain-Kontakte aktiviert ist, wird die E-Mail zur Bestätigung der Übertragung von identity-protect.org-Adressen zugestellt, die bei TLDs Amazon Registrar registriert sind. Die zuständige Vergabestelle für Ihre TLD finden Sie unter Wie Sie Ihre Vergabestelle finden.

Die Informationen, die Sie von WHOIS-Abfragen ausblenden können, hängen von zwei Faktoren ab:

Die Registrierung für die Top-Level-Domain

Die meisten TLD-Registrierungen blenden alle Kontaktinformationen automatisch aus, bei einigen können Sie wählen, ob alle Kontaktinformationen ausgeblendet werden sollen, und bei anderen können Sie nur einige oder gar keine Informationen ausblenden. Einige

TLD-Registries unterdrücken bewusst den Datenschutz, um den lokalen Vorschriften oder Registrierungsrichtlinien zu entsprechen.

Wenn der Datenschutz für eine Domain aktiviert ist, werden Ihre Kontaktinformationen entweder durch die Kontaktinformationen des Datenschutzservices oder durch den Satz „REDACTED FOR PRIVACY“ (AUS DATENSCHUTZGRÜNDEN UNKENNTLICH GEMACHT) ersetzt. Der Datenschutzdienst verwendet Funktionen zur Spam-Abwehr (Adressrotation und SPF/DKIM/spam Analyse) und leitet in den meisten Fällen E-Mails, die diese Filter passieren, automatisch weiter. Es ist jedoch nicht ratsam, vertrauliche E-Mails an datengeschützte E-Mail-Adressen zu senden, da der Spam-Mechanismus die Weiterleitung verhindern könnte.

Darüber hinaus ist die Wahl, welcher Datenschutzmechanismus für eine Domain verwendet wird, nicht konfigurierbar und wird vom System automatisch ausgewählt. Die Kontaktdaten für unseren Datenschutzservice können nicht manuell aktualisiert werden.

> **Note**
>
> Zur Aktivierung oder Deaktivierung des Datenschutzes für einige Domains müssen Sie einen Support-Fall eröffnen und Datenschutz anfordern. Weitere Informationen finden Sie im entsprechenden Abschnitt unter Domains, die Sie mit Amazon Route 53 registrieren können.
>
> - .co.uk (Großbritannien und Nordirland)
> - .me.uk (Großbritannien und Nordirland)
> - .org.uk (Großbritannien und Nordirland)
> - .link

Die Vergabestelle

Wenn Sie eine Domain mit Route 53 registrieren oder eine Domain in Route 53 übertragen, ist die Vergabestelle für die Domain entweder die Amazon-Vergabestelle oder unser Registrierungspartner Gandi. Die Amazon-Vergabestelle und Gandi blenden standardmäßig unterschiedliche Informationen aus:

- Amazon-Vergabestelle – Standardmäßig werden alle Ihre Kontaktinformationen ausgeblendet. Die Vorschriften für die TLD-Registrierung haben jedoch Vorrang.

- Gandi – Standardmäßig werden alle Ihre Kontaktinformationen ausgeblendet, außer dem Organisationsnamen, falls vorhanden. Die Vorschriften für die TLD-Registrierung haben jedoch Vorrang.

  In Regionen TLDs, in denen der Datenschutz nicht möglich ist, werden Ihre personenbezogenen Daten auf der Suchseite des Whois-Verzeichnisses auf der Gandi-Website als „geschwärzt“ gekennzeichnet. Ihre personenbezogenen Informationen können jedoch bei der Registrierung der Domäne oder auf WHOIS-Websites von Dritten verfügbar sein.

Welche Informationen für die TLD für Ihre Domäne ausgeblendet wurden, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können heraus.

Wenn Sie Datenschutz für eine Domäne aktivieren oder deaktivieren möchten, die Sie mit Route 53 registriert haben, führen Sie die folgenden Schritte aus.

> **Important**
>
> Verfügbarkeit des Datenschutzes: Datenschutz ist nicht für alle verfügbar. TLDs
> Zu den gängigen Anbietern TLDs , die den Datenschutz nicht unterstützen,
> gehören .de, .us, .com.au, .es und viele andere.
> Wenn Sie bei der Bearbeitung der Kontaktinformationen Ihrer Domain keinen Abschnitt „Datenschutz“ sehen, wird der Datenschutz für die TLD Ihrer Domain nicht unterstützt.
> Eine vollständige Liste der Anbieter TLDs , die den Datenschutz nicht unterstützen, finden Sie unterTLDs die den Datenschutz nicht unterstützen. Ausführliche Informationen zur Unterstützung des Datenschutzes für alle TLDs finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können.

So aktivieren oder deaktivieren Sie den Datenschutz für Kontaktinformationen für eine Domäne

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie den Namen der Domäne aus, deren Datenschutz Sie aktivieren oder deaktivieren möchten.
4. Wählen Sie im Abschnitt Kontaktinformationen die Option Bearbeiten aus.

5. Wählen Sie im Abschnitt Datenschutz aus, ob Kontaktinformationen ausgeblendet werden sollen. Sie müssen für alle vier Kontakte dieselbe Datenschutzeinstellung angeben: Administrator, Registrant, Techniker und Rechnungsstellung.

   > **Note**
   >
   > Wenn der Abschnitt Datenschutz nicht angezeigt wird, wird der Datenschutz für die TLD Ihrer Domain nicht unterstützt. Ihre Kontaktinformationen werden in WHOIS-Abfragen für Domains, die den Datenschutz nicht unterstützen, öffentlich sichtbar sein.

6. Wählen Sie Änderungen speichern aus.
7. Wenn Sie beim Aktivieren oder Deaktivieren des Datenschutzes auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

TLDs die den Datenschutz nicht unterstützen

Im Folgenden wird der Datenschutz TLDs nicht unterstützt. Wenn Ihre Domain eine dieser Optionen verwendet TLDs, sind Ihre Kontaktinformationen in WHOIS-Abfragen öffentlich sichtbar:

Generisch TLDs

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

Geografisch TLDs

.cl (Chile), .com.ar (Argentinien), .com.au (Australien), .com.br (Brasilien), .com.sg (Singapur), .de (Deutschland), .es (Spanien), .in (Indien), .net.au (Australien), .qa (Katar), .ru (Russland), .sg (Singapur), .us (Vereinigte Staaten), .vg (Britische Jungferninseln)

> **Note**
>
> Diese Liste enthält die häufigsten TLDs , die den Datenschutz nicht unterstützen. Vollständige up-to-date Informationen und Informationen zur Unterstützung des Datenschutzes für eine bestimmte TLD finden Sie auf der jeweiligen TLD-Seite unter. Domains, die Sie mit Amazon Route 53 registrieren können

Behebung von Datenschutzproblemen

Die Option zum Schutz der Privatsphäre ist in der Konsole nicht verfügbar

Dies weist darauf hin, dass die TLD Ihrer Domain keinen Datenschutz unterstützt. Ihre Kontaktinformationen werden in WHOIS-Abfragen öffentlich sichtbar sein. Dies ist TLDs aufgrund von Registrierungsrichtlinien oder lokalen Vorschriften mit Sicherheit ein normales Verhalten.

Um zu überprüfen, ob Ihre TLD den Datenschutz unterstützt, überprüfen Sie die jeweilige TLD-Seite unter Domains, die Sie mit Amazon Route 53 registrieren können oder unter. TLDs die den Datenschutz nicht unterstützen

Die Kontaktinformationen sind nach der Aktivierung des Datenschutzes weiterhin sichtbar

Einige Registries verwalten ihre eigenen WHOIS-Datenbanken und zeigen möglicherweise weiterhin Kontaktinformationen an, auch wenn der Datenschutz bei Route 53 aktiviert ist. Dies wird von der TLD-Registrierung gesteuert, nicht von Route 53.

Darüber hinaus bieten einige TLD-Registries bewusst eingeschränkte Datenschutz- oder Redaktionsdienste für ihre Domains an.

Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne

Wenn Sie die Einstellung ändern möchten, ob Amazon Route 53 die Registrierung für eine Domain kurz vor dem Ablaufdatum automatisch verlängert, oder die aktuelle Einstellung für die automatische Verlängerung sehen möchten, führen Sie die folgenden Schritte durch.

Beachten Sie, dass Sie keine AWS Credits verwenden können, um die Gebühr für die Verlängerung der Registrierung für eine Domain zu bezahlen.

> **Note**
>
> Stellen Sie sicher, dass Sie die automatische Verlängerung deaktivieren, wenn Sie Ihr AWS -Konto kündigen möchten. Andernfalls erhalten Sie weiterhin Verlängerungsmitteilungen von AWS. Ihre Domain wird allerdings nur verlängert, wenn Sie Ihr Konto reaktivieren.

So aktivieren oder deaktivieren Sie die automatische Verlängerung für eine Domäne

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Klicken Sie auf den Namen der Domäne, die Sie aktualisieren möchten.
4. Wählen Sie im Abschnitt Details in der Dropdownliste Aktionen die Option Automatische Verlängerung aktivieren aus.

   Stimmen Sie unter Automatische Verlängerung für <Domainname> aktivieren? der Zahlung des Jahrestarifs zu und wählen Sie Aktivieren aus.

   > **Note**
   >
   > Der angegebene Preis gilt für den aktuellen Registrierungszeitraum und kann sich ändern. Weitere Informationen finden Sie unter Amazon-Route-53-Preise für die Domainregistrierung.

5. Wenn Sie die automatische Verlängerung deaktivieren möchten, wählen Sie in der Dropdownliste Aktionen die Option Automatische Verlängerung deaktivieren aus.
6. Wenn bei der Aktivierung oder Deaktivierung der automatischen Verlängerung Probleme auftreten, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Sperren einer Domäne zum Verhindern der nicht autorisierten Übertragung an eine andere Vergabestelle

Mit den Domainregistrierungen für alle generischen TLDs und viele geografische Regionen können TLDs Sie eine Domain sperren, um zu verhindern, dass jemand die Domain ohne Ihre Zustimmung an einen anderen Registrar überträgt. Unter Domains, die Sie mit Amazon Route 53 registrieren können erfahren Sie, wie Sie bestimmen können, ob Ihnen die Registrierung für Ihre Domain erlaubt, die Domain zu sperren. Wenn die Sperrung unterstützt wird und Sie Ihre Domäne sperren möchten, führen Sie die folgenden Schritte aus. Sie können diesen Vorgang auch verwenden, um die Sperrung aufzuheben, wenn Sie eine Domäne an eine andere Vergabestelle übertragen möchten.

So sperren Sie eine Domäne, um die nicht autorisierte Übertragung an eine andere Vergabestelle zu verhindern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Registered Domains.
3. Klicken Sie auf den Namen der Domäne, die Sie aktualisieren möchten.
4. Wählen Sie im Bereich Details in der Dropdownliste Aktionen die Option Übertragungssperre aktivieren oder Übertragungssperre deaktivieren aus (je nachdem, ob Sie die Übertragungssperre ein- oder ausschalten möchten).

   Sie können zur Seite Anforderungen navigieren, um sich den Status Ihrer Anforderung anzusehen.
5. Wenn Sie beim Sperren einer Domain auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

In der WHOIS-Suche wird dieser Status wie folgt angezeigt: `clientTransferProhibited`. Manche haben TLDs möglicherweise zusätzlich diesen Status:

- `clientUpdateProhibited`
- `clientDeleteProhibited`

Verlängern des Registrierungszeitraums für eine Domäne

Wenn Sie eine Domain mit Amazon Route 53 registrieren oder die Domainregistrierung an Route 53 übertragen, wird die Domain mit automatischer Verlängerung konfiguriert. Die automatische Verlängerungsfrist beträgt in der Regel ein Jahr, obwohl die Registries für einige Top-Level-Domains (TLDs) längere Verlängerungszeiträume haben.

Beachten Sie Folgendes:

Maximaler Verlängerungszeitraum

Bei allen generischen TLDs und vielen Ländercodes können Sie TLDs die Domainregistrierung um längere Zeiträume verlängern, in der Regel um bis zu zehn Jahre in Schritten von einem Jahr. Informationen dazu, ob Sie den Registrierungszeitraum für Ihre Domäne verlängern können,

finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können. Wenn ein längerer Registrierungszeitraum zulässig sind, führen Sie die folgenden Schritte aus.

Einschränkungen für die Erneuerung oder Verlängerung einer Domänenregistrierung

Einige TLD-Registrierungen haben Einschränkungen, wann Sie eine Domänenregistrierung erneuern oder verlängern können, z. B. die letzten zwei Monate vor Ablauf der Domäne. Auch wenn die Registrierung die Verlängerung des Registrierungszeitraums für eine Domäne erlaubt, kann es an der aktuellen Anzahl von Tagen liegen, bevor die Domäne abläuft.

> **Note**
>
> Wenn der maximal zulässige Verlängerungszeitraum für die Domain, für die Sie Ihre Domain haben TLDs , beispielsweise 5 Jahre beträgt, können Sie jederzeit jährliche Verlängerungen hinzufügen, bis Sie das 5-Jahres-Limit erreicht haben. Genauer gesagt, wenn Sie eine Domain haben, die derzeit 2,5 Jahre gültig ist, können Sie sie nur um bis zu 2 weitere Jahre verlängern.

AWS Credits

Sie können AWS Credits nicht verwenden, um die Gebühr für die Verlängerung des Registrierungszeitraums für eine Domain zu bezahlen.

So verlängern Sie den Registrierungszeitraum für Ihre Domäne

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered Domains.
3. Wählen Sie den Namen der Domäne aus, für die Sie den Registrierungszeitraum verlängern möchten.
4. Wählen Sie im Abschnitt Details in der Dropdownliste Aktionen die Option Domainregistrierung verlängern aus.
5. Wählen Sie im Dialogfeld Domainregistrierung verlängern in der Dropdownliste Verlängerungszeitraum die Anzahl der Jahre aus, um die Sie die Registrierung verlängern möchten.

Die Liste enthält alle aktuellen Optionen basierend auf dem aktuellen Ablaufdatum und den maximalen Registrierungszeitraum, der laut Registrierung für diese Domäne zulässig ist. Das Ablaufdatum mit dieser Anzahl von Jahren ist unter der Dauer angegeben.

6. Wählen Sie Domainregistrierung verlängern aus.

   Wenn wir die Bestätigung von der Registrierung erhalten, dass sie das Ablaufdatum aktualisiert haben, senden wir Ihnen eine E-Mail, um zu bestätigen, dass das Ablaufdatum geändert wurde.

7. Wenn Sie bei der Verlängerung des Registrierungszeitraums für eine Domain auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelle

Wenn Sie die DNS-Verwaltung auf eine andere Vergabestelle umstellen möchten, müssen Sie die Namenserver aktualisieren, auf die verwiesen wird.

So aktualisieren Sie die Namensserver für Ihre Domäne, wenn Sie einen anderen DNS-Service verwenden möchten

1. Verwenden Sie den Prozess, der von Ihrem DNS-Service bereitgestellt wird, um die Namensserver für die Domäne abzurufen.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
4. Wählen Sie den Namen der Domäne aus, die Sie für einen anderen DNS-Service konfigurieren möchten.
5. Wählen Sie im Abschnitt Details in der Dropdownliste Aktionen die Option Namenserver bearbeiten aus.
6. Löschen Sie die vorhandenen Namenserver und fügen Sie dann die Namen der Namenserver zu den Namenservern hinzu, die Sie in Schritt 1 von Ihrem DNS-Service erhalten haben.
7. Wählen Sie Änderungen speichern aus.

8. (Optional) Löschen Sie die gehostete Zone, die Route 53 automatisch erstellt hat, als Sie Ihre Domäne registriert haben. Auf diese Weise wird verhindert, dass Sie Gebühren für eine gehostete Zone zahlen, die Sie nicht verwenden.

   a. Klicken Sie im Navigationsbereich auf Hosted Zones.
   b. Wählen Sie das Optionsfeld für die gehostete Zone aus, die denselben Namen hat wie Ihre Domäne.
   c. Wählen Sie Delete Hosted Zone.
   d. Klicken Sie auf Confirm, um zu bestätigen, dass Sie die gehostete Zone löschen möchten.

Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne

Wenn Sie eine Domain bei Route 53 registrieren, erstellen wir automatisch eine gehostete Zone für die Domain, weisen der gehosteten Zone vier Namenserver zu und aktualisiert dann die Domainregistrierung zur Verwendung dieser Namenserver. Diese Einstellungen müssen in der Regel nicht geändert werden, es sei denn, Sie möchten einen anderen DNS-Service oder White Label-Nameserver verwenden.

Die maximale Anzahl von Namenservern pro Domain in Route 53 ist 6.

> **Warning**
>
> Wenn Sie Namenserver auf den falschen Wert ändern, die falsche IP-Adresse in Glue-Datensätzen angeben oder einen oder mehrere Namenserver löschen, ohne neue anzugeben, ist Ihre Website oder Anwendung für bis zu zwei Tage nicht mehr im Internet verfügbar.

Themen

Überlegungen zum Ändern der Nameserver und Glue-Datensätze

Berücksichtigen Sie die folgenden Punkte, bevor Sie Ihre Konfiguration ändern.

Topics

Sie möchten Route 53 zum DNS-Service für Ihre Domäne machen

Wenn Sie derzeit einen anderen DNS-Service verwenden und Route 53 zum DNS-Service für Ihre Domäne machen möchten, finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen detaillierte Anweisungen zur Migration des DNS-Services in Route 53.

> **Important**
>
> Wenn Sie den Migrationsprozess nicht konsequent verfolgen, kann Ihre Domäne bis zu zwei Tage lang im Internet nicht verfügbar sein.

Wenn Sie einen anderen DNS-Service verwenden möchten

Wenn Sie einen anderen DNS-Service Route 53 für Ihre Domäne verwenden möchten, gehen Sie wie folgt vor, um die Nameserver für die Domänenregistrierung in die Namenserver zu ändern, die vom anderen DNS-Service bereitgestellt werden.

> **Note**
>
> Wenn Sie Namenserver und Route 53 ändern, wird die folgende Fehlermeldung angezeigt: Die Registrierungsstelle für die TLD erkennt die Namensserver nicht, die Sie als gültige Namenserver angegeben haben:
> `"We're sorry to report that the operation failed after we forwarded your request to our registrar associate. This is because: One or more of the specified name servers are not known to the domain registry."`
> TLD-Registries unterstützen in der Regel Nameserver, die von öffentlichen DNS-Diensten bereitgestellt werden, aber keine privaten DNS-Server, wie DNS-Server, die Sie auf EC2

Amazon-Instances konfiguriert haben, es sei denn, die Registry hat IP-Adressen für diese Nameserver. Route 53 unterstützt nicht die Verwendung von Namenservern, die von der TLD-Registrierung nicht erkannt werden. Wenn dieser Fehler auftritt, müssen Sie für Route 53 zu Nameservern oder einem anderen öffentlichen DNS-Service wechseln.

Wenn Sie White-Label-Server verwenden möchten

Wenn Sie möchten, dass die Namen Ihrer Nameserver Subdomänen Ihres Domänennamens werden, können Sie White Label-Nameserver erstellen. (White Label-Nameserver werden auch Vanity-Nameserver oder private Nameserver genannt.) Sie können beispielsweise Nameserver ns1.example.com durch ns4.example.com für die Domäne example.com erstellen. Für die Verwendung von White Label-Nameservern gehen Sie wie folgt vor, um die IP-Adressen für Ihre Namenserver anstelle der Namen anzugeben. Diese IP-Adressen werden als Glue-Datensätze bezeichnet.

Weitere Informationen zum Konfigurieren von White Label-Nameservern finden Sie unter Konfigurieren von White-Label-Nameservern.

Sie ändern Namenserver für eine .it-Domäne

IName Server für Ihre IT-Domain müssen eine DNS-Prüfung bestehen. Wir empfehlen Ihnen, die Nameserver unter https://dns-check.nic.it/, bevor Sie den Änderungsantrag einreichen. Die Registry reagiert weiterhin unter Verwendung der Nameserver von vor der Änderung auf DNS-Abfragen. Wenn die vorherigen Nameserver nicht mehr verfügbar sind, ist Ihre Domäne nicht mehr im Internet verfügbar.

> **Important**
>
> Wenn Sie Nameserver für eine Domäne ändern, müssen Sie stets sicherstellen, dass DNS mit den neuen Nameservern auf Abfragen reagiert, bevor Sie den alten DNS-Service abbrechen oder die gehostete Route-53-Zone löschen, die die alten Nameserver nutzte.

Informationen darüber, wie Sie Hilfe bei AWS der Korrektur der Namen Ihrer Nameserver bei der Registry für.it-Domains erhalten, finden Sie unterWenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Hinzufügen oder Ändern der Nameserver oder Glue-Datensätze

Wenn Sie Namenserver oder Glue-Datensätze hinzufügen oder ändern möchten, führen Sie die folgenden Schritte aus.

> **Note**
>
> Standardmäßig speichern DNS-Auflösungen die Namen von Namensservern normalerweise zwei Tage lang. Folglich kann es zwei Tage dauern, bis Ihre Änderungen wirksam werden. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

So können Sie Namenserver oder Glue-Datensätze für eine Domäne hinzufügen oder ändern

1. Überprüfen Sie Überlegungen zum Ändern der Nameserver und Glue-Datensätze und gehen Sie entsprechende Probleme an, falls vorhanden.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
4. Wählen Sie den Namen der Domäne aus, für die Sie die Einstellungen bearbeiten möchten.
5. Wählen Sie im Abschnitt Details in der Dropdownliste Aktionen die Option Namenserver bearbeiten aus.
6. Im Dialogfeld Namenserver bearbeiten haben Sie folgende Möglichkeiten:

   - Führen Sie einen der folgenden Schritte aus, um den DNS-Service für die Domäne zu ändern:
     - Ersetzen der Nameserver für einen anderen DNS-Service mit den Namenservern für eine gehostete Route-53-Zone
     - Ersetzen der Nameserver für eine gehostete Route-53-Zone mit den Nameservern für einen anderen DNS-Service
     - Ersetzen der Nameserver für eine Route-53-gehostete-Zone mit den Nameservern für eine andere Route-53-gehostete-Zone

   Weitere Informationen zum Ändern des DNS-Services für eine Domäne finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen. Informationen zum Abrufen der Namenserver für die gehostete Route-53-Zone, die Sie für den DNS-Service

für die Domäne verwenden möchten, finden Sie unter Das Abrufen der Nameserver für eine öffentliche gehostete Zone.

- Fügen Sie einen oder mehrere Namensserver hinzu.
- Ersetzen Sie den Namen eines vorhandenen Namensservers.
- Wenn Sie White-Label-Namenserver angeben, fügen Sie die IP-Adressen in Glue-Records hinzu oder ändern Sie diese. Sie können Adressen im IPv4 oder IPv6 -Format eingeben. Wenn ein Namensserver mehrere IP-Adressen hat, geben Sie jede Adresse in einer separaten Zeile ein.

  Ein White-Label-Namenserver beinhaltet Ihren Domänennamen, wie beispielsweise example.com, im Namen des Nameservers, wie z.B. ns1.example.com. Wenn Sie einen White-Label-Namenserver angeben, fordert Route 53 Sie auf, eine oder mehrere IP-Adressen für den Namenserver anzugeben. Diese IP-Adresse wird als Glue-Datensatz bezeichnet. Weitere Informationen finden Sie unter Konfigurieren von White-Label-Nameservern.
- Löschen Sie einen Namensserver. Klicken Sie auf das x-Symbol auf der rechten Seite des Feldes für den Namensserver.

> **Warning**
>
> Wenn Sie Namenserver auf den falschen Wert ändern, die falsche IP-Adresse in Glue-Datensätzen angeben oder einen oder mehrere Namenserver löschen, ohne neue anzugeben, ist Ihre Website oder Anwendung für bis zu zwei Tage nicht mehr im Internet verfügbar.

7. Wählen Sie Aktualisieren aus.
8. Wenn Sie beim Hinzufügen oder Ändern von Nameservern oder Glue-Datensätzen auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Verlängern der Registrierung für eine Domain

Wenn Sie eine Domain bei Amazon Route 53 registrieren oder die Domainregistrierung an Route 53 übertragen, wird die Domain mit automatischer Verlängerung konfiguriert. Der automatische Verlängerungszeitraum beträgt in der Regel ein Jahr, obwohl die Registries für einige Top-Level-Domains (TLDs) längere Verlängerungszeiträume haben. Informationen zum Registrierungs-

und Verlängerungszeitraum für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

> **Note**
>
> Sie können AWS Guthaben nicht verwenden, um die Gebühr für die Verlängerung der Registrierung einer Domain zu bezahlen.

Bei den meisten Top-Level-Domains (TLDs) können Sie das Ablaufdatum für eine Domain ändern. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

> **Important**
>
> Wenn Sie die automatische Verlängerung deaktivieren, beachten Sie die folgenden Auswirkungen für Ihre Domain:
>
> - Einige TLD-Registrierungen löschen Domains schon vor dem Ablaufdatum, wenn Sie nicht früh genug verlängern. Wir empfehlen Ihnen ausdrücklich, dass Sie die automatische Verlängerung aktiviert lassen, wenn Sie einen Domainnamen behalten möchten.
> - Wir empfehlen außerdem, nicht mit der erneuten Registrierung einer Domain nach deren Ablauf zu planen. Einige Vergabestellen ermöglichen es anderen, Domains sofort zu registrieren, nachdem eine Domain abgelaufen ist, sodass Sie ggf. nicht in der Lage sind, Ihre Domain erneut zu registrieren, bevor die Domain von jemand anderem genutzt wird.
> - Einige Registrierungsstellen berechnen eine hohe Gebühr, um abgelaufene Domains wiederherzustellen.
> - Am oder schon vor dem Ablaufdatum ist die Domain nicht mehr im Internet verfügbar.

Um zu bestimmen, ob die automatische Verlängerung für Ihre Domain aktiviert ist, finden Sie weitere Informationen unter Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne.

Wenn die automatische Verlängerung aktiviert ist, geschieht Folgendes:

45 Tage vor Ablauf

Wir senden eine E-Mail an den Registrierenden, um mitzuteilen, dass die automatische Verlängerung derzeit aktiviert ist. Diese enthält Anweisungen zum Deaktivieren. Halten Sie die E-Mail-Adresse des Registrierenden aktuell, sodass Sie diese E-Mail nicht verpassen.

35 oder 30 Tage vor Ablauf

Für alle Domains außer .com.ar- und .com.br-Domains verlängern wir die Domainregistrierung 35 Tage vor dem Ablaufdatum, sodass wir Zeit haben, alle Probleme mit Ihrer Verlängerung zu lösen, bevor der Domainname abläuft.

Die Registries für.com.ar- und .com.br-Domains verlangen, dass wir die Domains nicht mehr als 30 Tage vor Ablauf erneuern. Sie erhalten 30 Tage vor dem Ablaufdatum eine Verlängerungs-E-Mail von unserer Partner-Vergabestelle Gandi. Dabei handelt es sich um denselben Tag, an dem wir Ihre Domain verlängern, wenn die automatische Verlängerung aktiviert ist.

> **Note**
>
> Sobald wir Ihre Domain verlängern, senden wir Ihnen eine E-Mail, um Ihnen mitzuteilen, dass wir verlängert haben. Wenn die Verlängerung fehlgeschlagen ist, senden wir Ihnen eine E-Mail, um zu erläutern, warum sie fehlgeschlagen ist.

Wenn die automatische Verlängerung deaktiviert ist, passiert bei Annäherung des Ablaufdatums für einen Domainnamen Folgendes:

45 Tage vor Ablauf

Wir senden eine E-Mail an den Registrierenden für die Domain, um mitzuteilen, dass die automatische Verlängerung derzeit deaktiviert ist. Diese enthält Anweisungen zum Aktivieren. Halten Sie die E-Mail-Adresse des Registrierenden aktuell, sodass Sie diese E-Mail nicht verpassen.

30 Tage und 7 Tage vor Ablauf

Wenn die automatische Verlängerung für die Domain deaktiviert ist, verlangt ICANN (das Verwaltungsorgan für die Domainregistrierung), dass die Registrierungsstelle Ihnen eine E-Mail sendet. Die E-Mail kommt von einer der folgenden E-Mail-Adressen:

- noreply@registrar.amazon — Für Domains, für die der Registrar Amazon Registrar ist.
- noreply@domainnameverification.net oder noreply@emailverification.info — Für Domains, für die der Registrar unser Registrar-Mitarbeiter Gandi ist.

Die zuständige Vergabestelle für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

Wenn Sie die automatische Verlängerung weniger als 30 Tage vor Ablauf aktivieren und der Verlängerungszeitraum noch nicht vorbei ist, verlängern wir die Domain innerhalb von 24 Stunden.

> **Important**
>
> Bei einigen TLD-Registern gibt es Einschränkungen, wann Sie eine Domain verlängern können. Einzelheiten zu Ihrer Domain finden Sie unter. Domains, die Sie mit Amazon Route 53 registrieren können Darüber hinaus kann die Bearbeitung einer Verlängerung bis zu einem Tag dauern. Wenn Sie zu lange warten, bevor Sie die automatische Verlängerung aktivieren, kann die Domain vor der Bearbeitung der Verlängerung ablaufen, und es ist möglich, dass Sie die Domain verlieren. Wenn sich das Ablaufdatum nähert, empfehlen wir, dass Sie den Ablauftermin für die Domain manuell verlängern. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

Weitere Informationen zu Verlängerungszeiträumen finden Sie im Abschnitt „Fristen für die Verlängerung und Wiederherstellung von Domains“ für Ihre TLD in Domains, die Sie mit Amazon Route 53 registrieren können.

Nach dem Ablaufdatum

Die meisten Domains werden nach ihrem Ablauf noch eine Weile von der Vergabestelle vorgehalten, sodass Sie eine abgelaufene Domain möglicherweise auch nach dem Ablaufdatum noch verlängern können. Wir empfehlen jedoch dringend, die automatische Verlängerung aktiviert zu lassen, wenn Sie Ihre Domain behalten wollen. Weitere Informationen über die Verlängerung einer Domain nach dem Ablaufdatum finden Sie unter Wiederherstellen einer abgelaufenen oder gelöschten Domain.

Wenn eine Domain abläuft, für die Domain aber eine späte Verlängerung zulässig ist, können Sie die Domain zum Standardverlängerungspreis verlängern. Um zu ermitteln, ob sich eine Domain noch im Zeitraum für späte Verlängerung befindet, führen Sie die Schritte im Abschnitt Verlängern des Registrierungszeitraums für eine Domäne durch. Wenn die Domain noch aufgelistet ist, befindet sie sich im Zeitraum für späte Verlängerung.

Weitere Informationen zu Verlängerungszeiträumen finden Sie im Abschnitt „Fristen für die Verlängerung und Wiederherstellung von Domains“ für Ihre TLD in Domains, die Sie mit Amazon Route 53 registrieren können.

Wiederherstellen einer abgelaufenen oder gelöschten Domain

Wenn Sie eine Domain nicht vor Ablauf der späten Verlängerungsfrist verlängern oder wenn Sie die Domain versehentlich löschen, können Sie bei einigen Registraturen für Top-Level-Domains (TLDs) die Domain wiederherstellen, bevor sie für andere registriert werden kann.

Wenn eine Domain gelöscht wird oder das Ende des Zeitraums für späte Verlängerung überschritten wird, wird sie in der Amazon Route 53-Konsole nicht mehr angezeigt.

> **Important**
>
> Der Preis für die Wiederherstellung einer Domain ist in der Regel höher und gelegentlich deutlich höher als der Preis zum Registrieren oder Verlängern einer Domain. Den aktuellen Preis für die Wiederherstellung einer Domain finden Sie unter Amazon-Route-53-Preise für die Domainregistrierung in der Spalte mit dem Wiederherstellungspreis.

Sie können keine AWS Credits verwenden, um die Gebühr für die Wiederherstellung einer abgelaufenen Domain zu bezahlen.

So können Sie versuchen, eine Domainregistrierung nach dem Löschen oder nach Ablauf des Zeitraums für späte Verlängerung einer Domain wiederherzustellen

1. Bestimmen Sie, ob die TLD-Registrierungsdatenbank der betreffenden Domain die Wiederherstellung von Domains unterstützt und – falls dies der Fall ist – in welchem Zeitraum eine Wiederherstellung zulässig ist.

   a. Wechseln Sie zu Domains, die Sie mit Amazon Route 53 registrieren können.

      > **Important**
      >
      > Für generische TLD-Domains, die innerhalb der ersten 5 Tage nach der Registrierung gelöscht werden, gilt die standardmäßige 30-tägige Einlösefrist (Informationen zur tatsächlichen Anzahl der Tage finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können) nicht. Stattdessen stehen diese Domains sofort für eine neue Registrierung zur Verfügung.

   b. Suchen Sie nach der TLD für Ihre Domain und überprüfen Sie die Werte im Abschnitt mit den Fristen für die Verlängerung und Wiederherstellung von Domains.

> **Important**
>
> Wir leiten Wiederherstellungsanforderungen an Gandi weiter. Dort werden die Anforderungen während der Geschäftszeiten von Montag bis Freitag bearbeitet. Gandi hat seinen Sitz in Paris, wo die Zeit UTC/GMT +1 Stunde beträgt. Daher kann es in seltenen Fällen dazu kommen, je nachdem, wann Sie die Anfrage einreichen, dass es eine Woche dauern kann, bis die Anfrage bearbeitet wurde.

2. Der Preis für die Wiederherstellung einer Domain ist in der Regel höher und gelegentlich deutlich höher als der Preis zum Registrieren oder Verlängern einer Domain. Suchen Sie unter Amazon-Route-53-Preise für die Domainregistrierung nach der TLD für Ihre Domain (z. B. „.com“) und überprüfen Sie den Preis in der Spalte mit dem Wiederherstellungspreis. Wenn Sie die Domain weiterhin wiederherstellen möchten, notieren Sie sich den Preis. Sie benötigen ihn in einem späteren Schritt.
3. Melden Sie sich mit dem AWS Konto, für das die Domain registriert wurde, beim AWS Support Center an.
4. Geben Sie die folgenden Werte an:

   Regarding

   Akzeptieren Sie den Standardwert für Konto und Abrechnung.

   Service

   Akzeptieren Sie den Standardwert von Domains.

   Kategorie

   Akzeptieren Sie den Standardwert Restoration.

   Schweregrad

   Akzeptieren Sie den Standardwert für Allgemeine Frage.

   Klicken Sie auf Next step (Nächster Schritt): Additional information (Zusätzliche Informationen)

Betreff

Geben Sie Restore an expired domain (Abgelaufene Domain wiederherstellen) oder Restore a deleted domain (Gelöschte Domain wiederherstellen) ein.

Description

Geben Sie die folgenden Informationen ein:

- Die wiederherzustellende Domain
- Die 12-stellige Konto-ID des AWS Kontos, für das die Domain registriert wurde
- Bestätigung, dass Sie dem Preis zum Wiederherstellen der Domain zustimmen. Verwenden Sie den folgenden Text:

  „Ich stimme dem Preis von $ ____ für die Wiederherstellung meiner Domain zu.“

  Ersetzen Sie die Leerstelle durch den Preis, den Sie in Schritt 2 gefunden haben.

Kontaktmethode

Geben Sie eine Kontaktmethode an, und geben Sie die entsprechenden Werte ein.

5. Wählen Sie Absenden aus.
6. Wenn wir erfahren, ob wir Ihre Domain wiederherstellen konnten, wird sich ein AWS Support-Mitarbeiter mit Ihnen in Verbindung setzen. Wenn wir die Domain verlängern konnten, wird die Domain wieder in der Konsole angezeigt. Das Ablaufdatum hängt davon ab, ob die Domain abgelaufen ist oder versehentlich gelöscht wurde:

   Die Domain ist abgelaufen

   Das neue Ablaufdatum beträgt in der Regel ein oder zwei Jahre (abhängig von der TLD) nach dem alten Ablaufdatum.

   > **Note**
   >
   > Das neue Ablaufdatum wird nicht ab dem Datum berechnet, an dem die Domain wiederhergestellt wurde.

   Die Domain wurde versehentlich gelöscht

   Das Ablaufdatum ändert sich in der Regel nicht.

Ersetzen der gehosteten Zone für eine Domain, die bei Route 53 registriert ist

Wenn Sie die gehostete Zone für eine Domain löschen, müssen Sie eine andere gehostete Zone erstellen, wenn Sie bereit sind, die Domain im Internet zur Verfügung zu stellen. Führen Sie die folgenden Schritte aus.

Ersetzen der gehosteten Zone für eine Domain

1. Erstellen Sie eine öffentliche gehostete Zone. Weitere Informationen finden Sie unter Erstellen einer öffentlichen gehosteten Zone.
2. Erstellen von Datensätzen in der gehosteten Zone. Datensätze legen fest, wie Sie den Datenverkehr für die Domain (example.com) und Subdomains (acme.example.com, zenith.example.com) weiterleiten möchten. Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.
3. Aktualisieren Sie die Domainkonfiguration, um die Namensserver für die neue gehostete Zone zu verwenden. Weitere Informationen finden Sie unter Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

   > **Important**
   >
   > Wenn Sie eine gehostete Zone erstellen, weist Route 53 der gehosteten Zone einen Satz von vier Namensservern zu. Wenn Sie eine gehostete Zone löschen und anschließend eine gehostete Zone erstellen, weist Route 53 einen anderen Satz von vier Namenservern zu. Normalerweise stimmt keiner der Namensserver für die neue gehostete Zone mit einem der Namensserver für die vorherige gehostete Zone überein. Wenn Sie die Domainkonfiguration nicht aktualisieren, um die Namensserver für die neue gehostete Zone zu verwenden, steht die Domain im Internet weiterhin nicht zur Verfügung.

4. Wenn Sie beim Ersetzen der Hosting-Zone für eine Domain auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Übertragen von Domänen

Sie können die Domainregistrierung von einer anderen Vergabestelle an Amazon Route 53 übertragen, von einem AWS -Konto zu einem anderen oder von Route 53 zu einer anderen Vergabestelle. Für die Übertragung von Domains von einem AWS Konto auf ein anderes fallen keine Kosten an.

Die Themen in diesem Abschnitt behandeln die folgenden Themen im Zusammenhang mit der Übertragung von Domains:

1. Wählen Sie Ihre Transferart
   - Machen Sie sich mit dem Unterschied zwischen der Übertragung der Domainregistrierung auf Route 53 und der ausschließlichen Verwendung von Route 53 für DNS-Hosting vertraut.
   - Erfahren Sie anhand Ihrer Ziele in Bezug auf Domainverwaltung und DNS-Hosting, welche Option für Ihre Bedürfnisse am besten geeignet ist.
2. Checkliste vor der Übertragung
   - Führen Sie wichtige Vorbereitungsschritte durch, bevor Sie Ihre Domain auf Route 53 übertragen, um häufige Übertragungsfehler zu vermeiden.
   - Überprüfen Sie die Domain-Eignung, holen Sie sich Autorisierungscodes und bereiten Sie Ihre DNS-Einstellungen für einen reibungslosen Übertragungsprozess vor.
3. Übertragen der Registrierung für eine Domain an Amazon Route 53
   - Lernen Sie das step-by-step Verfahren für die Übertragung einer Domain von einem anderen Registrar zu Route 53 kennen, einschließlich der Voraussetzungen, Autorisierungscodes und der Aktualisierung der DNS-Einstellungen.
   - Erfahren Sie, wie sich die Übertragung einer Domain auf das Ablaufdatum auswirkt und welche Überlegungen für verschiedene Top-Level-Domains () TLDs zu beachten sind.
4. Häufige Übertragungsprobleme
   - Vermeiden Sie häufige Übertragungsprobleme, indem Sie sich mit den Domainanforderungen, Autorisierungsprozessen und zeitlichen Überlegungen vertraut machen.
   - Erfahren Sie, wie Sie Übertragungsprobleme lösen können und was zu tun ist, wenn Ihre Übertragung verzögert oder abgelehnt wird.
5. Überträgt eine Domain von Amazon Route 53 zu einer anderen Vergabestelle.
   - Machen Sie sich mit dem Prozess der Übertragung einer Domain von Route 53 zu einem anderen Registrar vertraut, einschließlich des Abrufs des Autorisierungscodes, der Aktualisierung der DNS-Einstellungen und der Beantwortung von Bestätigungs-E-Mails.

- Beachten Sie die Überlegungen bei der Übertragung des DNS-Dienstes an einen anderen Anbieter und die möglichen Auswirkungen auf Route 53-spezifische Funktionen wie Aliaseinträge und Routing-Richtlinien.

6. Übertragung einer Domain auf ein anderes AWS Konto
   - Erfahren Sie, wie Sie eine Domain von einem AWS Konto auf ein anderes übertragen, einschließlich der Rollen und Berechtigungen, die für die Initiierung und Annahme der Übertragung erforderlich sind.
   - Erfahren Sie mehr über den optionalen Schritt, die Hosting-Zone nach der Domainübertragung auf das neue Konto zu migrieren.
7. Status der Übertragung
   - Erfahren Sie, wie Sie den Status einer Domainübertragungsanfrage und die Bedeutung der verschiedenen Statuscodes während des Übertragungsvorgangs einsehen können.
8. Wie sich das Übertragen einer Domain an Amazon Route 53 auf das Ablaufdatum in der Domainregistrierung auswirkt
   - Erfahren Sie, wie sich die Übertragung einer Domain auf Route 53 auf das Ablaufdatum der Domain auswirken kann.

Wenn Sie die Informationen in den oben aufgeführten Themen befolgen, können Sie Domains effektiv zu und von Route 53 übertragen, den Übertragungsprozess verwalten und einen reibungslosen Übergang sicherstellen, während Sie gleichzeitig die richtige DNS-Konfiguration und das korrekte DNS-Routing beibehalten.

Wählen Sie Ihren Route 53-Übertragungstyp

Wenn Sie Amazon Route 53 mit Ihrer Domain verwenden möchten, haben Sie zwei Möglichkeiten. Wenn Sie den Unterschied verstehen, können Sie den richtigen Ansatz für Ihre Bedürfnisse wählen:

Übertragen Sie die Domainregistrierung auf Route 53

Mit dieser Option wird Route 53 zu Ihrem Domain-Registrar. Das bedeutet, dass Sie Ihre Domainverlängerungen, Kontaktinformationen und DNS-Einstellungen vollständig über Route 53 verwalten.

Wählen Sie diese Option, wenn Sie:

- Konsolidieren Sie Domainverwaltung und DNS-Hosting an einem Ort

- Nutzen Sie die Domänenverwaltungsfunktionen von Route 53
- Vereinfachen Sie die Abrechnung, indem Sie Domainverlängerungen auf Ihrer AWS Rechnung haben

Was Sie erwartet:

- Bearbeitungszeit: 5-7 Tage
- Voraussetzungen: Autorisierungscode des aktuellen Registrars, Domain entsperren, E-Mail-Adresse des Registranten verifizieren
- Wen Sie für Verlängerungen bezahlen: Route 53

Nächster Schritt: Füllen Sie das ausCheckliste vor der Übertragung für Domainübertragungen, um die Übertragung vorzubereiten.

Verwenden Sie Route 53 nur für DNS-Hosting

Mit dieser Option behalten Sie Ihren aktuellen Domain-Registrar, verwenden aber Route 53 als Ihren DNS-Dienst.

Wählen Sie diese Option, wenn Sie:

- Behalten Sie Ihr bestehendes Registrar-Verhältnis bei
- Verwenden Sie die erweiterten DNS-Funktionen von Route 53, ohne die Registrare zu wechseln
- Schneller Einstieg mit minimalen Voraussetzungen

Was ist zu erwarten:

- Zeit bis zur Fertigstellung: Bis zu 2 Tage (abhängig von der DNS-Verbreitung)
- Voraussetzungen: Keine
- Wen Sie für Verlängerungen bezahlen: Ihr derzeitiger Registrar

Nächster Schritt: Gehen Sie zu, Konfigurieren von Amazon Route 53 als DNS-Service um das DNS-Hosting einzurichten.

> **Important**
>
> Sie müssen Ihre Domainregistrierung nicht übertragen, um Route 53 als Ihren DNS-Dienst verwenden zu können. Sie können Ihren bestehenden Registrar behalten und Route 53 nur für DNS-Hosting verwenden.

Checkliste vor der Übertragung für Domainübertragungen

Bevor Sie mit der Übertragung Ihrer Domainregistrierung auf Amazon Route 53 beginnen, führen Sie die folgenden Prüfungen durch, um häufige Übertragungsfehler zu vermeiden und einen reibungslosen Ablauf zu gewährleisten.

Entscheiden Sie, was Sie übertragen möchten

Wählen Sie die Option, die Ihren Bedürfnissen entspricht:

Übertragen Sie die Domainregistrierung auf Route 53

Ihr Registrar wird Amazon Route 53. Sie zahlen Route 53 für Domainverlängerungen und verwalten die Domain-Einstellungen über die Route 53-Konsole.

Nächster Schritt: Fahren Sie mit dieser Checkliste fort und folgen Sie dann den Anweisungen. Übertragen der Registrierung für eine Domain an Amazon Route 53

Verwenden Sie Route 53 nur für DNS-Hosting

Behalten Sie Ihren aktuellen Registrar bei, verwenden Sie jedoch Route 53-Nameserver für die DNS-Auflösung. Sie zahlen weiterhin Ihren derzeitigen Registrar für Verlängerungen.

Nächster Schritt: Überspringen Sie diese Checkliste und folgen Sie ihnen. Konfigurieren von Amazon Route 53 als DNS-Service

Checkliste für die Voraussetzungen

Führen Sie alle folgenden Schritte aus, bevor Sie mit der Domainübertragung beginnen.

Checkliste vor der Übertragung (Füllen Sie alle Punkte aus)

1. ☐ Überprüfen Sie den E-Mail-Zugriff des Registranten

Bestätigen Sie, dass Sie E-Mails an die E-Mail-Adresse des Registranten erhalten können, da dieser die E-Mail zur Autorisierung der Domainübertragung erhält.

> **Important**
>
> Wenn Sie nicht auf die aktuelle E-Mail-Adresse des Registranten zugreifen können, aktualisieren Sie die E-Mail-Adresse für den Registranten, wenden Sie sich an Ihren aktuellen Registrar und warten Sie 60 Tage, bevor Sie die Übertragung vornehmen.

2. ☐ Domain entsperren

   Greifen Sie auf Ihre aktuellen Registrar-Domain-Einstellungen zu und deaktivieren Sie den Schutz „Domain Lock“ oder „Transfer Lock“, falls aktiviert.

   > **Note**
   >
   > Warten Sie nach dem Deaktivieren der Sperre einige Minuten, bis die Änderung wirksam wird, bevor Sie mit der Übertragung beginnen.

3. ☐ Besorgen Sie sich den Autorisierungscode

   Fordern Sie bei Ihrem aktuellen Registrar einen Autorisierungscode (Authentifizierungscode) an und wahren Sie dessen Vertraulichkeit. Sie geben diesen Code später im Übertragungsprozess in der Route 53-Konsole ein.

4. ☐ Überprüfen Sie das Alter und die Eignung der Domain

   Bestätigen Sie, dass Ihre Domain die ICANN-Transferanforderungen erfüllt:

   - Die Domain muss seit der ersten Registrierung mindestens 60 Tage alt sein.
   - Wenn die Domainregistrierung abgelaufen ist und wiederhergestellt wurde, muss sie vor mindestens 60 Tagen wiederhergestellt worden sein.

   > **Tip**
   >
   > Die ICANN-Regeln können Übertragungen vorübergehend blockieren, wenn die Kontaktdaten des Registranten kürzlich aktualisiert wurden (z. B. wenn Sie Ihren Namen oder Ihre E-Mail-Adresse geändert haben). Bei einigen Registraren können Sie diese

Sperre deaktivieren. Erkundigen Sie sich bei Ihrem aktuellen Registrar, wenn Sie sich nicht sicher sind.

5. ☐ Bereiten Sie die Zahlungsmethode vor

   Stellen Sie sicher, dass Ihr AWS Konto über eine gültige Zahlungsmethode verfügt. Wenn Sie eine Domain auf Route 53 übertragen, variiert die Transfergebühr, die wir für Ihr AWS Konto erheben, je nach Top-Level-Domain.

   Aktuelle Preise finden Sie unter Route 53-Preise.

   > **Note**
   >
   > Sie können kein AWS Guthaben verwenden, um Domainübertragungen zu bezahlen. Route 53 erhebt die Überweisungsgebühr vor Beginn des Vorgangs und bietet eine sofortige Rückerstattung, falls die Übertragung fehlschlägt.

6. ☐ DNSSEC deaktivieren (falls aktiviert)

   Wenn DNSSEC derzeit bei Ihrem aktuellen Registrar aktiviert ist, deaktivieren Sie es vorübergehend, bevor Sie mit der Übertragung beginnen. Dadurch wird sichergestellt, dass die Übertragung ohne Probleme bei der DNS-Validierung abgeschlossen werden kann.

   Warum das wichtig ist:

   Wenn Sie eine Domain übertragen, werden die bei Ihrem aktuellen Registrar gespeicherten DNSSEC-Schlüssel (KSK/ZSK) und DS-Einträge nicht automatisch auf Route 53 übertragen. Wenn Sie DNSSEC erneut aktivieren, ohne diese Schlüssel in Route 53 neu zu konfigurieren, schlägt Ihre Domain möglicherweise die DNS-Validierung fehl.

   Sicherer Ansatz (empfohlen):

   1. Deaktivieren Sie DNSSEC bei Ihrem aktuellen Registrar, bevor Sie die Übertragung starten.
   2. Schließen Sie die Domainübertragung ab und erstellen Sie Ihre Route 53-Hosting-Zone (falls nicht bereits erstellt).
   3. Stellen Sie sicher, dass alle DNS-Einträge korrekt aufgelöst werden, wenn DNSSEC nicht aktiviert ist.
   4. Konfigurieren Sie DNSSEC in Route 53 mit den neuen Werten Ihrer Hosting-Zone. KSK/ZSK

5. Aktivieren Sie DNSSEC erneut, indem Sie den neuen DS-Eintrag bei Ihrem TLD-Registrar (jetzt Route 53) veröffentlichen.

> **Tip**
>
> Wenn Sie Ihre Domain übertragen und gleichzeitig eine neue Hosting-Zone in Route 53 erstellen, deaktivieren Sie DNSSEC vor der Übertragung und warten Sie dann, bis die Einrichtung der Hosting-Zone verifiziert ist und die DNS-Auflösung korrekt funktioniert. Nach der Bestätigung können Sie DNSSEC problemlos über die Konsole von Route 53 wieder aktivieren. Überprüfen Sie immer Ihre DNS-Konfiguration in Route 53, bevor Sie DNSSEC erneut aktivieren. Weitere Informationen zu DNSSEC mit Route 53 finden Sie unter. Konfigurieren von DNSSEC für eine Domäne

Optional: Übertragen Sie zuerst den DNS-Dienst

Erwägen Sie, Ihren DNS-Dienst auf Route 53 zu übertragen, bevor Sie die Domainregistrierung übertragen. Dieser Ansatz bietet die folgenden Vorteile:

- Reduziert das Risiko von Website- oder E-Mail-Ausfallzeiten während der Übertragung
- Ermöglicht es Ihnen, die DNS-Funktionalität von Route 53 zu testen, bevor Sie sich für die vollständige Übertragung entscheiden
- Stellt eine Fallback-Option bereit, falls bei der Domainübertragung Probleme auftreten

Informationen zur ersten Übertragung des DNS-Dienstes finden Sie unterKonfigurieren von Amazon Route 53 als DNS-Service.

Nächste Schritte

Nach dem Ausfüllen dieser Checkliste:

1. Folgen Sie dem step-by-step Übertragungsvorgang unterÜbertragen der Registrierung für eine Domain an Amazon Route 53.
2. Überwachen Sie Ihre E-Mails während des Übertragungsvorgangs auf Autorisierungsnachrichten.

Übertragen der Registrierung für eine Domain an Amazon Route 53

> **Important**
>
> Bei der Übertragung von länderspezifischen Top-Level-Domains (ccTLDs) auf Route 53, mit Ausnahme von .cc und .tv, werden Aktualisierungen des Eigentümerkontakts ignoriert und die Kontaktdaten des Besitzers aus der Registry verwendet. Sie können die Kontaktinformationen des Eigentümers aktualisieren, nachdem die Übertragung abgeschlossen ist. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne.

Wenn Sie die Registrierung für eine Domain an Amazon Route 53 übertragen möchten, verwenden Sie die in diesem Thema beschriebenen Verfahren.

Überblick über den Übertragungsprozess

Die Domainübertragung umfasst die folgenden wichtigen Schritte:

1. Vollständige Checkliste vor der Übertragung

   Überprüfen Sie die Voraussetzungen, um Übertragungsfehler zu vermeiden. Siehe Checkliste vor der Übertragung für Domainübertragungen.
2. Übertragung in der Route 53 53-Konsole anfordern

   Geben Sie den Domainnamen und den Autorisierungscode ein. Siehe Schritt 5: Anfordern der Übertragung.
3. Autorisieren Sie per E-Mail (Kundenaktion erforderlich)

   Klicken Sie auf den Autorisierungslink, der innerhalb von 5 Tagen an die E-Mail des Registranten gesendet wurde. Siehe Schritt 6: Klicken Sie auf den Link in den Bestätigungs- und Autorisierungs-E-Mails.
4. Warten Sie auf den Abschluss

   Die Übertragung wird automatisch abgeschlossen, sofern sie nicht vom aktuellen Registrar abgelehnt wird. Überwachen Sie den Status in der Konsole.

Die häufigsten Fehlerquellen

Im Folgenden finden Sie Lösungen für häufig auftretende Probleme:

- E-Mail nicht erhalten: Stellen Sie sicher, dass auf die E-Mail-Adresse des Registranten zugegriffen werden kann, und überprüfen Sie den Spam-Ordner
- Domain gesperrt: Entsperren Sie die Domain beim aktuellen Registrar, bevor Sie mit der Übertragung beginnen
- Ungültiger Authentifizierungscode: Fordern Sie einen neuen Autorisierungscode vom aktuellen Registrar an
- Verletzung der 60-Tage-Regel: 60-Tage-ICANN-Regel (Teilnahmefrist). Übertragungen werden innerhalb von 60 Tagen nach der ersten Registrierung oder einer Änderung des Kontakts des Registranten blockiert. Bei einigen Registraren ist eine Abmeldung vor der Änderung möglich. Fragen Sie gegebenenfalls Ihren aktuellen Registrar.

> **Important**
>
> Wenn Sie einen Schritt überspringen, ist Ihre Domäne möglicherweise nicht mehr im Internet verfügbar.

Beachten Sie Folgendes:

AWS Support kontaktieren

Wenn während der Übertragung einer Domäne Probleme auftreten, wenden Sie sich an den kostenlosen AWS -Support. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Ablaufdatum

Weitere Informationen darüber, wie sich die Übertragung der Domäne auf das aktuelle Ablaufdatum auswirkt, finden Sie unter Wie sich das Übertragen einer Domain an Amazon Route 53 auf das Ablaufdatum in der Domainregistrierung auswirkt.

Übertragungsgebühr

Wenn Sie eine Domain zu Route 53 übertragen, hängt die Transfergebühr, die wir für Ihr AWS Konto erheben, von der Top-Level-Domain wie .com oder .org ab. Weitere Informationen dazu finden Sie unter Route-53-Preise.

Sie können AWS Guthaben nicht verwenden, um die Gebühr, falls vorhanden, für die Übertragung einer Domain zu Route 53 zu zahlen.

> **Note**
>
> Route 53 berechnet die Gebühr für die Übertragung Ihrer Domäne, bevor wir mit dem Übertragungsvorgang beginnen. Wenn eine Übertragung aus irgendeinem Grund fehlschlägt, werden Ihrem Konto sofort die Kosten für die Übertragung gutgeschrieben.

Spezielle und Premium-Domänennamen

Bei TLD Registrierungen sind einigen Domainnamen spezielle oder Premium-Preise zugeordnet. Sie können eine Domäne nicht in Route 53 übertragen, wenn für die Domäne ein Spezial- oder Premium-Preis gilt.

Domänenkontingente

Die standardmäßige Höchstanzahl von Domains pro AWS Konto beträgt 20. Sie können ein höheres Kontingent anfordern. Weitere Informationen finden Sie unter Kontingente für Domänen.

Grenzwert für Namenserver

Die maximale Anzahl von Namenservern pro Domain in Route 53 ist 6.

Themen

Übertragungsanforderungen für Top-Level-Domains

Die meisten Domänenvergabestellen erzwingen Anforderungen zur Übertragung von Domänen an eine andere Vergabestelle. Der primäre Zweck dieser Anforderungen besteht darin, zu verhindern, dass Eigentümer von betrügerischen Domänen die Domänen wiederholt an verschiedene Vergabestellen übertragen. Die Anforderungen variieren, aber meist gelten die folgenden Anforderungen:

- Sie müssen entweder die Domäne bei der aktuellen Vergabestelle registriert haben oder die Registrierung für die Domäne vor mindestens 60 Tagen an die aktuelle Vergabestelle übertragen haben.
- Wenn die Registrierung für einen Domänennamen abgelaufen war und wiederhergestellt werden musste, muss sie mindestens 60 Tagen zuvor wiederhergestellt worden sein.
- Die Domäne darf keinen der folgenden Domänennamen-Statuscodes haben:
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - serverTransferProhibited
- Die Registrierungsstellen für einige Top-Level-Domains erlauben keine Übertragung, bis die Änderungen abgeschlossen sind, z. B. Änderungen des Domäneneigentümers.

Eine aktuelle Liste der Domainnamen-Statuscodes und eine Erläuterung der jeweiligen Bedeutung finden Sie auf der ICANN-Website unter dem Stichwort „EPP Statuscodes“. (Suchen Sie auf der ICANN-Website, Web-Suchvorgänge geben gelegentlich eine veraltete Version des Dokuments zurück.)

> **Note**
>
> ICANN ist die Organisation, die Richtlinien für die Registrierung und Übertragung von Domänennamen festlegt.

Sie können auch auf der Website für Whois nach Ihrem Domänennamen suchen, um Statuscodes und andere Informationen für Ihre Domäne anzuzeigen.

Schritt 1: Sicherstellen, dass Amazon Route 53 die Top-Level-Domain unterstützt

Siehe Domains, die Sie mit Amazon Route 53 registrieren können. Wenn die Top-Level-Domain für die Domain, die Sie übertragen möchten, auf der Liste steht, können Sie die Domain an Amazon Route 53 übertragen.

Wenn eine TLD nicht auf der Liste steht, können Sie die Domänenregistrierung derzeit nicht in Route 53 übertragen. Gelegentlich fügen wir der Liste weitere TLDs hinzu. Schauen Sie also noch einmal nach, ob wir Unterstützung für Ihre Domain hinzugefügt haben.

Schritt 2 (optional): Übertragen des DNS-Service an Amazon Route 53 oder an einen anderen DNS-Serviceanbieter

Warum zuerst die DNS-Übertragung

Einige Registrare stellen einen kostenlosen DNS-Service bereit, der möglicherweise deaktiviert wird, sobald sie eine Anfrage von Route 53 erhalten, die Registrierung der Domäne zu übertragen. Wenn Route 53 den DNS-Service für Ihre Domäne bereitstellen soll, lesen Sie Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Schritt 3: Ändern der Einstellungen bei der aktuellen Vergabestelle

Führen Sie mit der von Ihrem aktuellen Registrar bereitgestellten Methode für jede Domäne, die Sie übertragen möchten, die folgenden Schritte aus.

- 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)

Vergewissern Sie sich, dass die E-Mail-Adresse für den Registrierenden Ihrer Domäne auf dem neuesten Stand ist

> Wir senden eine E-Mail an diese E-Mail-Adresse, um eine Genehmigung für die Übertragung zu erhalten. Sie müssen auf den Link in der E-Mail klicken, um die Übertragung zu autorisieren. Wenn Sie nicht auf den Link klicken, müssen wir die Übertragung abbrechen.

> **Important**
>
> Der Kontakt, den Sie als Registrant angeben, hat gemäß der ICANN-Übertragungsrichtlinie bestimmte Rechte als registrierter Inhaber des Domainnamens. Die meisten Domains werden nach der Schließung Ihrer Domain gelöscht AWS-Konto (weitere Informationen finden Sie unterMein AWS Konto ist geschlossen oder dauerhaft geschlossen und meine Domain ist bei Route 53 registriert). Bleibt eine Domain jedoch weiterhin in einem geschlossenen Konto, kann der Kontakt, den Sie als Registrant angegeben haben, möglicherweise die Übertragung des Domainnamens an einen externen Registrar beantragen. Daher ist es wichtig, dass der von Ihnen aufgeführte Registranten-Kontakt entweder Sie selbst oder eine andere Person ist, der Sie im Hinblick auf verantwortungsbewusstes Handeln vertrauen.

Entsperren Sie die Domäne, sodass sie übertragen werden kann

ICANN, das Verwaltungsorgan für Domainregistrierungen, erfordert, dass Sie Ihre Domain vor der Übertragung entsperren.

Vergewissern Sie sich, dass der Domänenstatus eine Übertragung der Domäne zulässt

Weitere Informationen finden Sie unter Übertragungsanforderungen für Top-Level-Domains.

Deaktivieren Sie DNSSEC für die Domäne

Wenn Sie DNSSEC mit einer Domäne verwenden und die Domänenregistrierung auf Route 53 übertragen, müssen Sie zuerst DNSSEC beim ehemaligen Registrar deaktivieren. Führen Sie dann nach der Übertragung der Domänenregistrierung Schritte aus, um DNSSEC für die Domäne in Route 53 einzurichten. Route 53 unterstützt zwar DNSSEC für die Domänenregistrierung, jedoch nicht für DNSSEC. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

> **Important**
>
> Wenn Sie eine Domänenregistrierung auf Route 53 übertragen, während DNSSEC konfiguriert ist, werden auch die öffentlichen DNSSEC-Schlüssel übertragen. Wenn Sie den DNS-Service auf einen Anbieter übertragen, der DNSSEC nicht unterstützt, schlägt die DNS-Auflösung zeitweise fehl, bis Sie die DNSSEC-Schlüssel aus der Domäne

löschen. Weitere Informationen finden Sie unter Löschen von öffentlichen Schlüsseln für eine Domäne.

Abrufen eines Autorisierungscodes

Ein Autorisierungscode von der aktuellen Vergabestelle berechtigt uns, die Übertragung der Registrierung für die Domäne in Route 53 zu beantragen. Sie geben diesen Code zu einem späteren Zeitpunkt in die Route-53-Konsole ein.

Einige Top-Level-Domains (TLDs) haben zusätzliche Anforderungen:

.co.za-Domänen

Sie benötigen keinen Autorisierungscode, um eine .co.za-Domäne nach Route 53 zu übertragen.

Domänen .uk, .co.uk, .me.uk und .org.uk

Wenn Sie eine .uk-, .co.uk-, .me.uk- oder .org.uk-Domäne zu Route 53 übertragen, müssen Sie keinen Autorisierungscode abrufen. Verwenden Sie stattdessen die von Ihrer aktuellen Domains-Vergabestelle angegebene Methode, um den Wert des IPS-Tags für die Domain auf GANDI zu aktualisieren, komplett in Großbuchstaben. (Ein IPS-Tag ist für Nominet erforderlich, der Registrierungsstelle für .uk-Domainnamen.) Wenn Ihre Vergabestelle keine Möglichkeit bietet, den Wert des IPS-Tags zu ändern, wenden Sie sich an Nominet.

Beachten Sie Folgendes beim Ändern des IPS-Tags:

Sie müssen die Übertragung innerhalb von fünf Tagen anfordern.

Wenn Sie die Übertragung nicht innerhalb von fünf Tagen nach dem Ändern des IPS-Tags anfordern, ändert sich das Tag wieder auf den vorherigen Wert. Sie müssen den Wert des IPS-Tags erneut ändern, andernfalls schlägt die Übertragungsanforderung fehl.

Anzeigen des IPS-Tags in WHOIS-Abfragen

Die Änderung am IPS-Tag wird erst in WHOIS-Abfragen angezeigt, nachdem die Übertragung an Route 53 abgeschlossen ist.

E-Mail von Gandi

Möglicherweise erhalten Sie eine E-Mail von unserem Vergabestellenpartner Gandi über den Übertragungsprozess. Wenn Sie eine E-Mail von Gandi (transfer-auth@gandi.net)

über die Übertragung Ihrer Domain erhalten, ignorieren Sie die Anweisungen in der E-Mail, da sie für Domains.uk, .co.uk, .me.uk oder .org.uk nicht relevant sind. Befolgen Sie stattdessen die Anweisungen in diesem Thema.

Erneuern Sie Ihre Domainregistrierung, bevor Sie die Domain übertragen (geografisch ausgewählt) TLDs

In den meisten TLDs Fällen wird die Registrierung bei der Übertragung einer Domain automatisch um ein Jahr verlängert. In einigen Regionen wird die Registrierung TLDs jedoch nicht verlängert, wenn Sie die Domain übertragen. Wenn Sie eine Domain auf Route 53 übertragen, die über eine dieser Optionen verfügt TLDs, empfehlen wir Ihnen, die Domainregistrierung zu erneuern, bevor Sie die Domain übertragen, insbesondere wenn sich das Ablaufdatum nähert.

> **Important**
>
> Wenn Sie die Domäne vor der Übertragung nicht verlängern, läuft möglicherweise die Registrierung ab, bevor die Übertragung abgeschlossen ist. Wenn dies geschieht, ist die Domäne im Internet nicht mehr verfügbar, während der Name der Domäne zum Kauf durch andere Personen verfügbar werden könnte.

Die Registrierung wird nicht automatisch verlängert, wenn Sie die folgenden Domänen an eine andere Vergabestelle übertragen:

- .ch (Schweiz)
- .cl (Chile)
- .co.uk (Großbritannien und Nordirland)
- .co.za (Südafrika)
- .com.au (Australien)
- .cz (Tschechische Republik)
- .es (Spanien)
- .fi (Finnland)
- .im (Isle of Man)
- .jp (Japan)
- .me.uk (Großbritannien und Nordirland)
- .net.au (Australien)

- .org.uk (Großbritannien und Nordirland)
- .se (Schweden)
- .uk (Großbritannien und Nordirland)

Schritt 4: Abrufen der Namen Ihrer Nameserver

Wenn Sie Amazon Route 53 als DNS-Service verwenden oder den vorhandenen DNS-Service weiter nutzen, rufen wir die Namen der Namensserver später im Prozess automatisch für Sie ab. Fahren Sie mit Schritt 5: Anfordern der Übertragung fort.

Wenn Sie den DNS-Service zu einem anderen Anbieter als Route 53 ändern möchten, während Sie die Domäne an Route 53 übertragen, verwenden Sie das Verfahren des DNS-Service-Anbieters, um die Namen der Namensserver für jede Domäne abzurufen, die Sie übertragen möchten.

> **Important**
>
> Wenn die Vergabestelle für Ihre Domäne auch der DNS-Service-Anbieter für die Domäne ist, übertragen Sie Ihren DNS-Service an Route 53 oder einen anderen DNS-Anbieter, bevor Sie den Prozess zur Übertragung der Domänenregistrierung fortsetzen.
> Wenn Sie den DNS-Service zusammen mit der Domänenregistrierung übertragen, sind Ihre Website, E-Mail und die Webanwendungen, die mit der Domäne verknüpft sind, möglicherweise nicht mehr verfügbar. Weitere Informationen finden Sie unter Schritt 2 (optional): Übertragen des DNS-Service an Amazon Route 53 oder an einen anderen DNS-Serviceanbieter.

Schritt 5: Anfordern der Übertragung

Um die Domainregistrierung von der aktuellen Vergabestelle in Amazon Route 53 zu übertragen, verwenden Sie die Route-53-Konsole, um die Übertragung zu beantragen. Route 53 übernimmt die Kommunikation mit der aktuellen Vergabestelle für die Domäne.

Sie können die Konsole verwenden, um bis zu fünf Domains zu übertragen.

Das verwendete Verfahren ist davon abhängig, ob Sie eine einzelne Domain oder bis zu fünf Domains übertragen möchten:

- So übertragen Sie die Domainregistrierung einer einzelnen Domain an Route 53

- So übertragen Sie die Domainregistrierung für bis zu fünf Domänen an Route 53

Verwenden Sie den Prozess Domain auf Ihr Konto übertragen, um eine einzelne Domain an Ihr Konto zu übertragen.

So übertragen Sie die Domainregistrierung einer einzelnen Domain an Route 53

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie auf der Seite Registrierte Domains in der Dropdownliste Übertragung in die Option Einzelne Domain aus.
4. Geben Sie auf der Seite Domain auf Ihr Konto übertragen im Abschnitt Domain-Übertragbarkeit überprüfen den Namen der Domain ein, deren Registrierung Sie an Route 53 übertragen möchten, und wählen Sie Prüfen aus.
5. Wenn die Domainregistrierung übertragen werden kann, vergewissern Sie sich, dass die Übertragungsanforderungen für Top-Level-Domains erfüllt sind, und wählen Sie Weiter aus.

   Wenn die Domänenregistrierung nicht für die Übertragung verfügbar ist, listet die Route-53-Konsole die Gründe auf. Wenden Sie sich an die Vergabestelle, um Informationen zum Beheben der Probleme zu erhalten, die verhindern, dass Sie die Registrierung übertragen können.
6. Überprüfen Sie auf der Seite DNS-Service die Informationen zu den Namenservern und wählen Sie Weiter aus.
7. Geben Sie bei entsprechender Aufforderung den Autorisierungscode oder das IPS-Tag ein, den bzw. das Sie von Ihrer aktuellen Vergabestelle unter Schritt 3: Ändern der Einstellungen bei der aktuellen Vergabestelle erhalten haben.

   > **Note**
   >
   > Sie müssen keinen Autorisierungscode eingeben, um eine.co.za-, .uk-, .co.uk-, .me.uk- oder .org.uk-Domain auf Route 53 zu übertragen.

   Wählen Sie Weiter aus.
8. Wählen Sie auf der Seite Preisoptionen für Domains aus, für wie viele Jahre Sie die zu übertragende Domain registrieren möchten und ob Ihre Domainregistrierung vor dem Ablaufdatum automatisch verlängert werden soll.

> **Note**
>
> Registrierungen und Verlängerungen von Domainnamen sind nicht erstattungsfähig. Wenn Sie die automatische Domainverlängerung aktivieren und entscheiden, dass Sie den Domainnamen nach der Verlängerung der Registrierung nicht mehr wünschen, können Sie die Kosten der Verlängerung nicht erstattet bekommen.

Wählen Sie Weiter aus.

9. Geben Sie auf der Seite mit den Kontaktinformationen die Kontaktinformationen für den Domainregistranten, den Administrator, die technischen Ansprechpartner und die Rechnungsstellung ein. Die Werte, die Sie hier eingeben, gelten für alle Domains, die Sie registrieren. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain.

   Beachten Sie die folgenden Überlegungen:

   Vorname und Nachname

   Wir empfehlen für First Name und Last Name den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen an den Domaineinstellungen erfordern manche Domainregistrierungen einen Identitätsnachweis. Der Name in Ihrer ID muss genau mit dem Namen des aktuellen Registrierenden der Domain übereinstimmen.

   Unterschiedliche Kontakte

   Standardmäßig verwenden wir die gleichen Informationen für alle drei Kontakte. Wenn Sie für einen oder mehrere der Kontakte andere Informationen eingeben möchten, deaktivieren Sie die Option Wie Registranten-Kontakt.

   > **Note**
   >
   > Bei Domains vom Typ „.it“ müssen Registranten-Kontakt und Administratorkontakt identisch sein.

Weitere erforderliche Informationen

Für einige Top-Level-Domains (TLDs) müssen wir zusätzliche Informationen sammeln. Geben Sie dafür die entsprechenden Werte nach dem Feld Postal/PLZ ein. TLDs

Datenschutz

Wählen Sie, ob Sie Ihre Kontaktinformationen vor WHOIS-Abfragen verbergen möchten.

> **Note**
>
> Für Administratorkontakt, Registranten-Kontakt und technischen Kontakt muss jeweils die gleiche Datenschutzeinstellung angegeben werden.

Weitere Informationen finden Sie unter den folgenden Themen:

- Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne
- Domains, die Sie mit Amazon Route 53 registrieren können

> **Note**
>
> Zur Aktivierung des Datenschutzes für Domains vom Typ „.uk“, „co.uk“, „.me.uk“ und „.org.uk“ müssen Sie einen Support-Fall erstellen und Datenschutz anfordern.

Wählen Sie Weiter aus.

10. Überprüfen Sie auf der Seite Überprüfen Ihre Angaben und korrigieren Sie sie gegebenenfalls. Lesen Sie die Servicevertragsbedingungen und aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bedingungen gelesen haben.

    Wählen Sie Submit request (Anforderung absenden) aus.

11. Wählen Sie im Navigationsbereich die Option Domains und anschließend Anforderungen aus.

    Auf dieser Seite können Sie sich den Status der Domain ansehen und auch ermitteln, ob Sie auf die Verifizierungs-E-Mail des Registranten-Kontakts antworten müssen. Außerdem können Sie die Verifizierungs-E-Mail erneut senden.

Wenn Sie eine E-Mail-Adresse für den Registranten-Kontakt angegeben haben, die noch nie zur Registrierung einer Domain bei Route 53 verwendet wurde, müssen Sie bei einigen TLD-Registrierungsstellen die Gültigkeit der Adresse bestätigen.

Anschließend wird eine Verifizierungs-E-Mail von einer der folgenden E-Mail-Adressen gesendet:

- noreply@registrar.amazon — für die TLDs Registrierung bei Amazon Registrar.
- noreply@domainnameverification.net oder noreply@emailverification.info — für die TLDs Registrierung durch unseren Registrar-Mitarbeiter Gandi. Die zuständige Vergabestelle für Ihre TLD finden Sie unter Wie Sie Ihre Vergabestelle finden.

> **Important**
>
> Der registrierende Kontakt muss die Anweisungen in der E-Mail befolgen, um zu bestätigen, dass die E-Mail-Adresse empfangen wurde. Andernfalls muss die Domain gesperrt werden, wie von ICANN gefordert. Wenn eine Domain gesperrt ist, kann im Internet nicht darauf zugegriffen werden.

a. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link in der E-Mail, um zu bestätigen, dass die E-Mail-Adresse gültig ist. Wenn Sie die E-Mail nicht sofort erhalten, überprüfen Sie Ihren Spam-Ordner.

b. Kehren Sie zur Seite Anforderungen zurück. Wenn der Status nicht automatisch aktualisiert wird und email-address is verified angezeigt wird, wählen Sie Refresh status.

12. Nach Abschluss der Domainübertragung hängt der nächste Schritt davon ab, ob Sie Route 53 oder einen anderen DNS-Service als DNS-Service für die Domain verwenden möchten:

    - Route 53 – In der gehosteten Zone, die Route 53 bei der Registrierung der Domain erstellt hat, erstellen Sie Datensätze und teilen Route 53 mit, wie der Datenverkehr für die Domain und Subdomains weitergeleitet werden soll.

      Wenn zum Beispiel jemand den Domainnamen in einen Browser eingibt und diese Abfrage an Route 53 weitergeleitet wird, möchten Sie, dass Route 53 die Abfrage mit der IP-Adresse eines Webservers in Ihrem Rechenzentrum oder mit dem Namen eines Elastic Load Balancing-Load Balancers beantwortet?

      Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

> **Important**
>
> Wenn Sie Datensätze in einer anderen gehosteten Zone erstellen als der, die Route 53 automatisch erstellt hat, müssen Sie die Nameserver für die Domain aktualisieren, sodass diese die Nameserver für die neue gehostete Zone verwenden.

- Ein anderer DNS-Service – Konfigurieren Sie Ihre neue Domain zum Weiterleiten von DNS-Abfragen an den anderen DNS-Service. Führen Sie das Verfahren unter Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelle aus.

Gehen Sie wie folgt vor, um bis zu fünf Domains an Ihr Konto zu übertragen.

So übertragen Sie die Domainregistrierung für bis zu fünf Domänen an Route 53

1. Öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie auf der Seite Registrierte Domains in der Dropdownliste Übertragung in die Option Mehrere Domains aus.
4. Geben Sie auf der Seite Übertragen mehrerer Domains in Ihr Konto bis zu fünf zu übertragende Domains sowie ggf. deren Autorisierungscode pro Zeile ein und wählen Sie anschließend Prüfen aus.
5. Wenn die Domainregistrierung übertragen werden kann, wird sie in der Liste Domainverfügbarkeit als verfügbar aufgeführt. Aktivieren Sie das Kontrollkästchen neben jeder Domain, deren Registrierung Sie übertragen möchten, vergewissern Sie sich, dass die Übertragungsanforderungen für Top-Level-Domains erfüllt sind, und wählen Sie Weiter aus.

   Wenn die Domänenregistrierung nicht für die Übertragung verfügbar ist, listet die Route-53-Konsole die Gründe auf. Wenden Sie sich an die Vergabestelle, um Informationen zum Beheben der Probleme zu erhalten, die verhindern, dass Sie die Registrierung übertragen können.
6. Überprüfen Sie auf der Seite DNS-Service die Informationen zu den Namenservern und wählen Sie Weiter aus.

> **Note**
>
> Registrierungen und Verlängerungen von Domainnamen sind nicht erstattungsfähig. Wenn Sie die automatische Domainverlängerung aktivieren und entscheiden, dass Sie

den Domainnamen nach der Verlängerung der Registrierung nicht mehr wünschen, können Sie die Kosten der Verlängerung nicht erstattet bekommen.

7. Geben Sie auf der Seite Kontaktinformationen die Kontaktinformationen für den Domain-Registranten, für den Administrator und für den technischen Kontakt an. Die Werte, die Sie hier eingeben, gelten für alle Domänen, die Sie übertragen.

> **Important**
>
> Es wird empfohlen, die folgenden Werte für den Registrantenkontakt (den Domänenbesitzer) anzugeben:
>
> - Bei Vor- und Nachname empfehlen wir den Namen so einzugeben, wie er in Ihrem offiziellen Ausweis lautet. Für einige Änderungen an den Domaineinstellungen erfordern manche Domainregistrierungen einen Identitätsnachweis. Der Name in Ihrer ID muss genau mit dem Namen des aktuellen Registrierenden der Domain übereinstimmen.
> - Kontaktdaten: Während der Domänenübertragung wird empfohlen, die gleichen Werte anzugeben, die bei der aktuellen Vergabestelle angegeben werden. Wenn Sie die Kontaktdaten für den registrierten Kontakt ändern, wird der Domänenbesitzers geändert. Einige TLD-Registrierungen ermöglichen es Ihnen nicht, den Domänenbesitzers während einer Domänenübertragung zu ändern. Wenn Sie die Kontaktdaten für den registrierten Kontakt ändern, schlägt die Übertragung möglicherweise fehl. Sie können die Kontaktdaten für den registrierten Kontakt ändern, nachdem Sie die Domäne übertragen haben.

Standardmäßig verwenden wir die gleichen Informationen für alle drei Kontakte. Wenn Sie für einen oder mehrere der Kontakte andere Informationen eingeben möchten, deaktivieren Sie die Option Wie Registranten-Kontakt.

> **Note**
>
> Bei Domains vom Typ „.it“ müssen Registranten-Kontakt und Administratorkontakt identisch sein.

Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain.

8. Bei TLDs einigen müssen wir zusätzliche Informationen sammeln. Geben Sie für diese TLDs Daten die entsprechenden Werte nach dem Feld PLZ/PLZ ein.
9. Wenn der Wert von Contact Type Person ist, geben Sie an, ob Sie Ihre Kontaktinformationen vor WHOIS-Abfragen verbergen möchten. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne.
10. Wählen Sie Absenden aus.
11. Überprüfen Sie die Informationen, die Sie eingegeben haben, lesen Sie die Servicevertragsbedingungen, und aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Bedingungen gelesen haben.
12. Wählen Sie Submit request (Anforderung absenden) aus.

    Wir bestätigen, dass die Domains zur Übertragung berechtigt ist, und wir senden eine E-Mail an die Registranten-Kontakte für die Domain, um eine Autorisierung für die Übertragung der Domain anzufordern.
13. Wählen Sie im Navigationsbereich die Option Domains und anschließend Anforderungen aus.

    Auf dieser Seite können Sie sich den Status der Domain ansehen und auch ermitteln, ob Sie auf die Verifizierungs-E-Mail des Registranten-Kontakts antworten müssen. Außerdem können Sie die Verifizierungs-E-Mail erneut senden.

    Wenn Sie eine E-Mail-Adresse für den Registranten-Kontakt angegeben haben, die noch nie zur Registrierung einer Domain bei Route 53 verwendet wurde, müssen Sie bei einigen TLD-Registrierungsstellen die Gültigkeit der Adresse bestätigen.

    Anschließend wird eine Verifizierungs-E-Mail von einer der folgenden E-Mail-Adressen gesendet:

    - noreply@registrar.amazon — für die TLDs Registrierung bei Amazon Registrar.
    - noreply@domainnameverification.net oder noreply@emailverification.info — für die TLDs Registrierung durch unseren Registrar-Mitarbeiter Gandi. Die zuständige Vergabestelle für Ihre TLD finden Sie unter Wie Sie Ihre Vergabestelle finden.

> **Important**
>
> Der registrierende Kontakt muss die Anweisungen in der E-Mail befolgen, um zu bestätigen, dass die E-Mail-Adresse empfangen wurde. Andernfalls muss die Domain gesperrt werden, wie von ICANN gefordert. Wenn eine Domain gesperrt ist, kann im Internet nicht darauf zugegriffen werden.

a. Wenn Sie die Bestätigungs-E-Mail erhalten, wählen Sie den Link in der E-Mail, um zu bestätigen, dass die E-Mail-Adresse gültig ist. Wenn Sie die E-Mail nicht sofort erhalten, überprüfen Sie Ihren Spam-Ordner.

b. Kehren Sie zur Seite Anforderungen zurück. Wenn der Status nicht automatisch aktualisiert wird und email-address is verified angezeigt wird, wählen Sie Refresh status.

14. Nach Abschluss der Domainübertragung hängt der nächste Schritt davon ab, ob Sie Route 53 oder einen anderen DNS-Service als DNS-Service für die Domain verwenden möchten:

- Route 53 – In der gehosteten Zone, die Route 53 bei der Registrierung der Domain erstellt hat, erstellen Sie Datensätze und teilen Route 53 mit, wie der Datenverkehr für die Domain und Subdomains weitergeleitet werden soll.

  Wenn zum Beispiel jemand den Domainnamen in einen Browser eingibt und diese Abfrage an Route 53 weitergeleitet wird, möchten Sie, dass Route 53 die Abfrage mit der IP-Adresse eines Webservers in Ihrem Rechenzentrum oder mit dem Namen eines ELB Load Balancers beantwortet?

  Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

  > **Important**
  >
  > Wenn Sie Datensätze in einer anderen gehosteten Zone erstellen als der, die Route 53 automatisch erstellt hat, müssen Sie die Nameserver für die Domain aktualisieren, sodass diese die Nameserver für die neue gehostete Zone verwenden.

- Ein anderer DNS-Service – Konfigurieren Sie Ihre neue Domain zum Weiterleiten von DNS-Abfragen an den anderen DNS-Service. Führen Sie das Verfahren unter Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelle aus.

Schritt 6: Klicken Sie auf den Link in den Bestätigungs- und Autorisierungs-E-Mails

Kurz danach, nachdem Sie die Übertragung beantragt haben, senden wir möglicherweise eine oder mehrere E-Mails an den Registranten-Kontakt für die Domäne:

E-Mail, um zu bestätigen, dass der Registranten-Kontakt erreichbar ist

Wenn Sie nie eine Domäne bei Route 53 registriert oder eine Domäne in übertragen haben, senden wir Ihnen eine E-Mail, um zu bestätigen, dass die E-Mail-Adresse gültig ist. Wir behalten diese Informationen bei, damit wir keine erneute Bestätigungs-E-Mail senden müssen.

E-Mail, um die Genehmigung zur Übertragung der Domäne zu erhalten.

Bei einigen TLDs müssen Sie auf eine E-Mail antworten, um die Übertragung der Domain zu autorisieren.

Generische Produkte TLDs wie .com, .net und .org

Für Domänen mit einer generischen TLD, wie z. B. .com, .net oder .org, ist keine Autorisierung erforderlich.

Geografisch TLDs wie .co.uk und .jp

Für Domänen, die eine geografische TLD haben, müssen wir Ihre Genehmigung für die Übertragung der Domäne einholen. Wenn Sie 10 Domänen übertragen, müssen wir 10 E-Mails an Sie senden, und Sie müssen in jeder davon auf den Autorisierungs-Link klicken.

Die E-Mails gehen alle an den Registranten-Kontakt für die Domäne:

- Wenn Sie der Registrierende für die Domäne sind, befolgen Sie die Anweisungen in der E-Mail, um die Übertragung zu autorisieren.
- Wenn jemand anders der Registrierende ist, bitten Sie denjenigen, die Anweisungen in der E-Mail zu befolgen, um die Übertragung zu autorisieren.

> **Important**
>
> Wenn Sie eine Domäne übertragen, die über eine geografische TLD verfügt, warten wir bis zu fünf Tage darauf, dass der Registranten-Kontakt die Übertragung genehmigt. Wenn der Registrierende nicht innerhalb von fünf Tagen reagiert, stornieren wir die Übertragung und

senden eine E-Mail an den Registrierenden, um ihn über die Stornierung in Kenntnis zu setzen.

Themen

Autorisierungs-E-Mail für einen neuen Eigentümer oder eine neue E-Mail-Adresse

Wenn Sie die folgenden Werte geändert haben, senden wir Ihnen zu Autorisierungszwecken eine separate E-Mail:

Domäneneigentümer

Wenn Sie den Eigentümer einer Domäne ändern, wie unter Was löst eine Änderung der Domaininhaberschaft aus? beschrieben, senden wir eine E-Mail an den Registrierenden für die Domäne.

E-Mail-Adresse für den Ansprechpartner des Registranten (nur für einige) TLDs

Wenn Sie die E-Mail-Adresse für den Kontakt mit dem Registranten ändern, senden wir in einigen TLDs Fällen eine E-Mail an die alte und die neue E-Mail-Adresse für den Kontakt mit dem Registranten. Jemand muss an beiden E-Mail-Adressen die Anweisungen in der E-Mail befolgen, um die Änderung zu autorisieren.

Wenn wir bei Änderungen am Domaineigentümer oder an der E-Mail-Adresse für den Registranten-Kontakt nicht innerhalb von 3 bis 15 Tagen (abhängig von der Top-Level-Domain) eine Autorisierung für die Änderung erhalten, müssen wir die Anforderung gemäß ICANN stornieren.

E-Mail-Adressen, von denen Autorisierungs-E-Mails gesendet werden

Alle E-Mails kommen von einer der folgenden E-Mail-Adressen.

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt
.com.au und .net.au	no-reply@ispapi.net Die E-Mail enthält einen Link zu http://transfers.ispapi.net.
.fr	nic@nic.fr, wenn Sie den Registrierenden für eine .fr-Domäne gleichzeitig mit der Domänenübertragung ändern möchten. (Die E-Mail wird sowohl an den aktuellen Registrierenden als auch an den neuen Registrierenden gesendet.)
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

Die zuständige Vergabestelle für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

Genehmigung der aktuellen Vergabestelle

Wenn der Registrierende die Übertragung autorisiert, beginnen wir zusammen mit Ihrer aktuellen Vergabestelle, Ihre Domäne zu übertragen. Dieser Schritt kann bis zu zehn Tagen dauern, abhängig von der TLD für Ihre Domäne:

- Generische Top-Level-Domains – brauchen bis zu sieben Tage
- Geografische Top-Level-Domains (auch als Ländercode-Domänen oberster Ebene bekannt) – brauchen bis zu zehn Tage

Wenn Ihre aktuelle Vergabestelle nicht auf unsere Übertragungsanfrage antwortet, was bei Vergabestellen häufig passiert, erfolgt die Übertragung automatisch. Wenn Ihre aktuelle Vergabestelle die Übertragungsanfrage ablehnt, senden wir eine E-Mail-Benachrichtigung an den

aktuellen Registrierenden. Der Registrierende muss sich direkt mit der aktuellen Vergabestelle in Verbindung setzen und die Probleme mit der Übertragung beheben.

Wie geht es weiter?

Wenn Ihre Domänenübertragung genehmigt wurde, senden wir eine weitere E-Mail an den Registrierenden. Weitere Informationen über den Prozess finden Sie unter Anzeigen des Status einer Domänenübertragung.

Wir belasten Ihr AWS Konto mit dem Domaintransfer, sobald der Transfer abgeschlossen ist. Eine Liste der Gebühren nach TLD finden Sie unter Amazon-Route-53-Preise für die Domainregistrierung.

> **Note**
>
> Dies ist eine einmalige Gebühr, sodass die Kosten nicht in Ihren CloudWatch-Abrechnungsmetriken erscheinen. Weitere Informationen zu CloudWatch Metriken finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Schritt 7: Aktualisieren Sie die Domain-Konfiguration

Nachdem die Übertragung abgeschlossen ist, können Sie optional die folgenden Einstellungen ändern:

Übertragungssperre

Zum Übertragen der Domäne in Route 53 mussten Sie die Übertragungssperre deaktivieren. Wenn Sie die Sperre zur Verhinderung von unautorisierten Übertragungen erneut aktivieren möchten, finden Sie weitere Informationen unter Sperren einer Domäne zum Verhindern der nicht autorisierten Übertragung an eine andere Vergabestelle.

Automatische Verlängerung

Wir konfigurieren die übertragene Domäne zum automatischen Verlängern, wenn sich das Ablaufdatum nähert. Weitere Informationen zum Ändern dieser Einstellungen finden Sie unter Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne.

Verlängerter Registrierungszeitraum

Standardmäßig erneuert Route 53 die Domäne jährlich. Wenn Sie die Domäne für einen längeren Zeitraum registrieren möchten, finden Sie weitere Informationen unter Verlängern des Registrierungszeitraums für eine Domäne.

DNSSEC

Weitere Informationen zur Konfiguration von DNSSEC für die Domäne finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Vermeidung häufiger Probleme bei der Übertragung von Route 53

Wenn Sie während der Domainübertragung auf Probleme stoßen, finden Sie hier die häufigsten Probleme und wie Sie sie lösen können:

> **Note**
>
> Falls Ihre Übertragung bereits fehlgeschlagen ist, finden Sie Informationen Übertragen meiner Domäne an Amazon Route 53 fehlgeschlagen zur Problembehebung nach einem Ausfall.

Sie haben die Autorisierungs-E-Mail nicht erhalten

Wenn Sie die Autorisierungs-E-Mail von Route 53 nicht erhalten, finden Sie hier die häufigsten Ursachen und Lösungen:

- Schauen Sie in Ihrem Spam-Ordner nach — Autorisierungs-E-Mails werden manchmal von E-Mail-Anbietern gefiltert.
- Bestätigen Sie Ihre E-Mail-Adresse — Vergewissern Sie sich, dass die E-Mail-Adresse des Registranten in den Kontaktinformationen Ihrer Domain aktuell und zugänglich ist.
- Aktualisieren Sie Ihre Kontaktinformationen — Wenn die E-Mail-Adresse veraltet ist, aktualisieren Sie sie bei Ihrem aktuellen Registrar, bevor Sie mit der Übertragung beginnen.
- Autorisierungs-E-Mail erneut senden — Klicken Sie in der Route 53-Konsole für die Domain im Übertragungsstatus auf „Autorisierungs-E-Mail erneut senden“.

Sie erhalten die Fehlermeldung „Ungültiger Autorisierungscode“

Wenn Sie die Fehlermeldung „Ungültiger Autorisierungscode“ erhalten, versuchen Sie es mit diesen Lösungen:

- Überprüfen Sie den Code noch einmal. Bei den Autorisierungscodes wird zwischen Groß- und Kleinschreibung unterschieden. Kopieren Sie den Code und fügen Sie ihn direkt von der Benutzeroberfläche Ihres Registrars ein, um Tippfehler zu vermeiden.
- Prüfen Sie, ob der Code abgelaufen ist. Autorisierungscodes können je nach aktuellem Registrar zwischen 5 und 30 Tagen ablaufen. Fordere einen neuen Code an, falls deiner abgelaufen ist.
- Überflüssige Leerzeichen entfernen — Achten Sie darauf, dass bei der Eingabe des Codes keine Leerzeichen am Anfang oder Ende stehen.
- Holen Sie sich einen neuen Autorisierungscode — Wenn der Code weiterhin fehlschlägt, fordern Sie bei Ihrem aktuellen Registrar einen neuen Autorisierungscode an.

Ihre Domain ist beim aktuellen Registrar gesperrt

Domainübertragungen können fehlschlagen, wenn Ihr derzeitiger Registrar eine Transfersperre aktiviert hat (auch bekannt als „Domainsperre“ oder „Kundenübertragung verboten“). Dies ist eine gängige Sicherheitseinstellung, die unbefugte Übertragungen verhindert.

So beheben Sie dieses Problem

- Entsperren Sie Ihre Domain — Loggen Sie sich in das Kontrollpanel Ihres aktuellen Registrars ein und deaktivieren Sie die Domainübertragungssperre.
- Stellen Sie sicher, dass die Sperre aufgehoben wurde — Sie können jedes öffentliche WHOIS-Suchtool verwenden, um zu überprüfen, ob der Domainstatus „OK“ statt „“ clientTransferProhibited anzeigt.
- Holen Sie sich Hilfe von Ihrem Registrar — Wenn Sie keine Option zum Entsperren Ihrer Domain sehen, wenden Sie sich an das Support-Team Ihres aktuellen Registrars. Sie können Ihnen helfen, die Sperre zu entfernen.

Ihre Domain ist nicht übertragbar

Wenn Ihr Domaintransfer aufgrund von Zulassungsproblemen abgelehnt wird, überprüfen Sie Folgendes:

- Überprüfen Sie das Domainalter — Ihre Domain muss seit der Registrierung oder letzten Übertragung mindestens 60 Tage alt sein.
- TLD-Unterstützung überprüfen — Vergewissern Sie sich, dass Route 53 die Top-Level-Domain (TLD) Ihrer Domain unterstützt. Informationen zur Unterstützung finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können. TLDs
- Domainstatus überprüfen — Domains mit bestimmten Statuscodes (wie „pendingTransfer“ oder „redemptionPeriod“) können nicht übertragen werden.

- Überprüfen Sie das Ablaufdatum — Domains, die abgelaufen sind oder innerhalb von 15 Tagen ablaufen, sind möglicherweise nicht übertragbar.
- Abrechnungsprobleme lösen — Vergewissern Sie sich, dass alle ausstehenden Gebühren bei Ihrem aktuellen Registrar bezahlt sind.

Ihre Übertragung dauert länger als erwartet

Wenn sich Ihre Übertragung zu verzögern scheint, sollten Sie Folgendes wissen:

- Normaler Zeitrahmen — Die meisten Übertragungen werden innerhalb von 5-7 Tagen abgeschlossen, können aber auch bis zu 10 Tage dauern.
- Übertragungsstatus überwachen — Überprüfen Sie Ihren Übertragungsfortschritt in der Route 53-Konsole. Weitere Informationen finden Sie unter Anzeigen des Status einer Domänenübertragung.
- Schnell auf E-Mails antworten — Beide Registrare senden Ihnen möglicherweise Bestätigungs-E-Mails, für deren Fortsetzung Ihre Antwort erforderlich ist.
- Wenden Sie sich an Ihren aktuellen Registrar — Wenn sich die Übertragung verzögert, wenden Sie sich an Ihren aktuellen Registrar, um sicherzustellen, dass er die Übertragung nicht blockiert.

Wann Sie den AWS Support kontaktieren sollten

Wenden Sie sich an den AWS Support, wenn Sie die oben genannten Lösungen ausprobiert haben und immer noch Probleme haben, oder wenn Sie auf Folgendes stoßen:

- Die Übertragung schlägt nach mehreren Versuchen mit korrekten Informationen fehl
- Abrechnungs- oder Zahlungsprobleme während des Übertragungsvorgangs
- Technische Fehler in der Route 53-Konsole, die Sie daran hindern, eine Übertragung zu starten
- Übertragungen, die länger als 10 Tage im Status „Ausstehend“ verbleiben

Wenn Sie sich an den Support wenden, geben Sie bitte Ihren Domainnamen, die ID der Übertragungsanfrage (falls verfügbar) und Einzelheiten zu dem spezifischen Fehler oder Problem an, das bei Ihnen aufgetreten ist.

Überträgt eine Domain von Amazon Route 53 zu einer anderen Vergabestelle.

Wenn Sie eine Domain von Amazon Route 53 an eine andere Vergabestelle übertragen, erhalten Sie einige Informationen von Route 53 für die neue Vergabestelle. Die neue Vergabestelle erledigt den Rest.

Important

Wenn Sie derzeit Route 53 als DNS-Service-Anbieter verwenden und den DNS-Service ebenfalls an einen anderen Anbieter übertragen möchten, sollten Sie daran denken, dass die folgenden Route-53-Funktionen keine direkten Entsprechungen mit Funktionen von anderen DNS-Service-Anbieter haben. Sie müssen mit dem neuen DNS-Service-Anbieter zusammenarbeiten, um zu bestimmen, wie Sie eine vergleichbare Funktionalität erzielen:

- Alias-Datensätze. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.
- Andere Routing-Richtlinien außer der einfachen Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.
- Die mit Datensätzen verknüpften Zustandsprüfungen. Weitere Informationen finden Sie unter Konfigurieren von DNS Failover.

Die meisten Domänenvergabestellen erzwingen Anforderungen zur Übertragung von Domänen an eine andere Vergabestelle. Der primäre Zweck dieser Anforderungen besteht darin, zu verhindern, dass Eigentümer von betrügerischen Domänen die Domänen wiederholt an verschiedene Vergabestellen übertragen. Die Anforderungen variieren, aber meist gelten die folgenden Anforderungen:

- Sie müssen die Domain vor mindestens 14 Tagen beim aktuellen Registrar registriert oder die Registrierung für die Domain auf den aktuellen Registrar übertragen haben.
- Die Domäne darf keinen der folgenden Domänennamen-Statuscodes haben:
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited

- serverTransferProhibited

Eine aktuelle Liste der Domainnamen-Statuscodes und eine Erläuterung, was jeder Code bedeutet, finden Sie auf der ICANN-Website unter dem Stichwort EPP Statuscodes. (Suchen Sie auf der ICANN-Website, Web-Suchvorgänge geben gelegentlich eine veraltete Version des Dokuments zurück.)

> **Note**
>
> Wenn Sie Ihre Domain zu einem anderen Domain-Registrar übertragen möchten, das AWS Konto, mit dem die Domain registriert ist, aber geschlossen, gesperrt oder gekündigt ist, können Sie sich an den AWS Support wenden, um Hilfe zu erhalten. Domains können innerhalb der ersten 14 Tage nach der Registrierung nicht übertragen werden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

> **Note**
>
> Wenn der neue Registrar einen REG-ID-Code benötigt, können Sie sich an den AWS Support wenden, um Hilfe zu erhalten. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

So übertragen Sie eine Domäne von Route 53 zu einer anderen Vergabestelle

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie den Namen der Domäne aus, die Sie an eine andere Vergabestelle übertragen möchten.
4. Überprüfen Sie auf der Seite Domainname den Wert für Domänennamen-Statuscode. Wenn es einer der folgenden Werte ist, können Sie die Domäne derzeit nicht übertragen:
   - pendingDelete
   - pendingTransfer

- redemptionPeriod
- clientTransferProhibited
- serverTransferProhibited

Eine aktuelle Liste der Domainnamen-Statuscodes und eine Erläuterung, was jeder Code bedeutet, finden Sie auf der ICANN-Website unter dem Stichwort EPP Statuscodes. (Suchen Sie auf der ICANN-Website, Web-Suchvorgänge geben gelegentlich eine veraltete Version des Dokuments zurück.)

Wenn der Wert des Domainnamen-Statuscodes lautet serverTransferProhibited, können Sie sich kostenlos an den AWS Support wenden, um zu erfahren, was Sie tun müssen, um die Domain zu übertragen. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

5. Wenn der Wert von Transfersperre auf Ein festgelegt ist, wählen Sie in der Dropdownliste Aktionen die Option Übertragungssperre deaktivieren aus.
6. Alle Domains außer den Domains.be-, .co.za-, .ru-, .uk-, .co.uk-, .me.uk- und .org.uk-Domains — Wählen Sie auf der Domainnamenseite im Drop-down-Menü Transfer out die Option Zu einem anderen Registrar übertragen aus.

   Wählen Sie im Dialogfeld An eine andere Vergabestelle übertragen die Option Kopieren aus, um den Autorisierungscode für die Domainübertragung zu kopieren. Sie müssen diesen Wert zu einem späteren Zeitpunkt in diesem Verfahren bei Ihrer Vergabestelle angeben.

   > **Note**
   >
   > Für .eu-Domains können Sie den Authentifizierungscode auch mithilfe des Fensters „Mein.eu“ in der Registry generieren: https://my.eurid.eu/.

   Domains.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk und .org.uk — Gehen Sie wie folgt vor:

   .be-Domains

   Holen Sie sich den Autorisierungscode von der Registry für.be-Domains auf der Website von DNS Belgien.

.co.za-Domänen

Sie benötigen keinen Autorisierungscode, um eine .co.za-Domäne auf eine andere Vergabestelle zu übertragen.

.ru-Domänen

Holen Sie sich den Autorisierungscode von der Registry für .ru-Domains unter https://www.nic. ru/en/auth/recovery/:

a. Wählen Sie die Option zur Wiederherstellung von Anmeldeinformationen nach Domänennamen.

b. Geben Sie den Domänennamen ein und wählen Sie Fortfahren.

c. Folgen Sie den Anweisungen auf dem Bildschirm, um Zugriff zur RU-CENTER-Administratorseite zu erhalten.

d. Wählen Sie im Abschnitt Manage your account (Verwalten Ihres Kontos) die Option Domain transfer (Domänenübertragung).

e. Bestätigen Sie die Übertragung mit REGRU-RU.

Domänen .uk, .co.uk, .me.uk und .org.uk

Ändern Sie das IPS-Tag auf den Wert für die neue Domänenvergabestelle:

a. Suchen Sie auf der Seite Find a Registrar der Nominet-Website den IPS-Tag für die neue Vergabestelle. (Nominet ist die Registrierungsstelle für .uk-, .co.uk-, .me.uk- und .org.uk-Domänen.)

b. Wählen Sie auf der Seite Registrierte Domains > Domainname das Drop-down-Menü Ausgehende Übertragung, dann IPS-Tag aktualisieren aus und geben Sie den Wert an, den Sie in Schritt 6a erhalten haben.

c. Wählen Sie Aktualisieren aus.

> **Note**
>
> Sie können das IPS-Tag auch in der Nominet-Konsole aktualisieren. Eine Anleitung dazu finden Sie unter Wechseln Sie den Registrar.

7. Wenn Sie derzeit nicht Route 53 als DNS-Service-Anbieter für Ihre Domäne verwenden, gehen Sie direkt zu Schritt 10.

Wenn Sie derzeit Route 53 als DNS-Service-Anbieter für die Domäne verwenden, führen Sie die folgenden Schritte aus:

a. Wählen Sie Hosted Zones (Gehostete Zonen) aus.

b. Wählen Sie den Namen der gehosteten Zone für Ihre Domäne. Die Domäne und die gehostete Zone haben denselben Namen.

c. Wenn Sie Route 53 weiterhin als DNS-Serviceanbieter für die Domäne verwenden möchten: Rufen Sie die Namen der vier Namensserver ab, die Route 53 Ihrer gehosteten Zone zugewiesen hat. Weitere Informationen finden Sie unter Das Abrufen der Nameserver für eine öffentliche gehostete Zone.

   Wenn Sie Route 53 nicht länger als DNS-Serviceanbieter für die Domäne verwenden möchten: Notieren Sie die Einstellungen für alle Ihre Datensätze außer den NS- und SOA-Datensätzen. Für Route-53-spezifische Funktionen wie Aliasdatensätze müssen Sie gemeinsam mit dem neuen DNS-Serviceanbieter herausfinden, wie eine vergleichbare Funktionalität erzielt werden kann.

8. Wenn Sie den DNS-Dienst an einen anderen Anbieter übertragen, verwenden Sie die Methoden des neuen DNS-Dienst, um die folgenden Aufgaben auszuführen:

   - Erstellen Sie eine gehostete Zone
   - Erstellen Sie Datensätze, die die Funktionalität Ihrer Route 53 Datensätze reproduzieren
   - Rufen Sie die Nameserver auf, die den neuen DNS-Dienst Ihrer gehosteten Zone zugewiesen haben

9. Fordern Sie mit dem Verfahren der neuen Vergabestelle eine Übertragung der Domäne an.

   Alle Domains außer den Domains.co.za, .uk, .co.uk, .me.uk und .org.uk — Sie werden aufgefordert, den Autorisierungscode einzugeben, den Sie in Schritt 6 dieses Verfahrens von der Route 53-Konsole erhalten haben.

10. Wenn Sie Route 53 weiterhin als DNS-Dienstanbieter verwenden möchten, verwenden Sie das vom neuen Registrar bereitgestellte Verfahren, um die Namen der Route 53-Nameserver anzugeben, die Sie in Schritt 7 erhalten haben. Wenn Sie einen anderen DNS-Dienstanbieter verwenden möchten, geben Sie die Namen der Nameserver an, die Ihnen der neue Anbieter beim Erstellen einer neuen Hostzone in Schritt 8 gegeben hat.

11. Beantworten Sie die Bestätigungs-E-Mail:

Alle Domänen außer .jp-Domänen

Route 53 sendet eine Bestätigungs-E-Mail an die E-Mail-Adresse für den Registrierenden der Domäne:

- Wenn Sie nicht auf die E-Mail antworten, erfolgt die Übertragung automatisch am angegebenen Datum.
- Wenn Sie möchten, dass die Übertragung früher oder gar nicht stattfindet, rufen Sie über den Link in der E-Mail die Route 53-Website auf und wählen Sie die entsprechende Option aus.
- Je nach TLD kann die Bestätigungs-E-Mail einen Link enthalten, über den https://approvemove.com Sie die Übertragung genehmigen oder ablehnen können. Wenn der Datenschutz für die Domain-Kontakte aktiviert ist, wird die E-Mail von identity-protect.org-Adressen zugestellt, die bei Amazon Registrar TLDs registriert sind. Die zuständige Vergabestelle für Ihre TLD finden Sie unter Wie Sie Ihre Vergabestelle finden.

.jp-Domänen

Route 53 sendet eine Bestätigungs-E-Mail an die E-Mail-Adresse des Registranten-Kontakts für die Domain von der Adresse noreply@domainnameverification.net oder noreply@emailverification.info mit einem Link zur Bestätigung der Übertragung:

- Wenn Sie nicht auf die E-Mail antworten, wird die Überweisung zum angegebenen Datum storniert.
- Wenn Sie möchten, dass die Übertragung früher oder gar nicht stattfindet, rufen Sie über den Link in der E-Mail die Route 53-Website auf und wählen Sie die entsprechende Option aus. Sie werden den Domänen-Autorisierungscode angeben müssen, den Sie in Schritt 7 erhalten haben.

Darüber hinaus erhalten Sie möglicherweise eine E-Mail von Wixi.jp. Sie können diese E-Mail ignorieren.

12. Wenn die Domänenvergabestelle, an die Sie die Domäne übertragen, einen Übertragungsfehler meldet, wenden Sie sich an diese Domänenvergabestelle, um weitere Informationen zu erhalten. Wenn Sie eine Domäne an eine andere Domänenvergabestelle übertragen, gehen alle Statusaktualisierungen an die neue Domänenvergabestelle, also verfügt Route 53 über keine Informationen zum Grund des Übertragungsfehlers.

    Wenn die neue Domänenvergabestelle meldet, dass die Übertragung fehlgeschlagen ist, weil der von Route 53 erhaltene Autorisierungscode ungültig ist, öffnen Sie einen Fall mit

dem AWS -Support. (Sie benötigen keinen Support-Vertrag und es wird keine Gebühr berechnet.) Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

> **Note**
>
> Von Gandi generierte Autorisierungscodes sind etwa 5 Tage gültig. Wenn Ihr Übertragungsversuch nach diesem Zeitraum erfolgt, schlägt er möglicherweise aufgrund eines abgelaufenen Codes fehl.

13. Wenn Sie den DNS-Service an einen anderen DNS-Serviceanbieter übertragen haben, können Sie die Datensätze in der gehosteten Zone sowie die gehostete Zone löschen, nachdem die DNS-Resolver keine DNS-Abfragen mit den Namen der Route-53-Namenservers mehr beantworten. Dies dauert in der Regel zwei Tage. Diese Zeit benötigen die DNS-Resolver in der Regel, um die Namen der Namenserver für eine Domäne zwischenzuspeichern.

> **Important**
>
> Wenn Sie die gehostete Zone löschen, während die DNS-Resolver immer noch auf DNS-Abfragen mit den Namen der Route-53-Namenserver antworten, ist Ihre Domäne im Internet nicht mehr verfügbar.

Nachdem Sie die gehostete Zone gelöscht haben, wird Ihnen die monatliche Gebühr für die gehostete Zone von Route 53 nicht mehr in Rechnung gestellt. Weitere Informationen finden Sie in der folgenden Dokumentation:

- Löschen von Datensätzen
- Löschen einer öffentlichen gehosteten Zone
- Route-53-Preise

Übertragung einer Domain auf ein anderes AWS Konto

Wenn Sie eine Domain mit einem AWS Konto registriert haben und die Domain auf ein anderes AWS Konto übertragen möchten, können Sie sie einfach mithilfe der neuen Konsole oder mithilfe der AWS CLI oder anderer programmatischer Methoden übertragen.

Themen

Schritt 1: Eine Domain auf ein anderes AWS Konto übertragen

Domains können innerhalb der ersten 14 Tage nach der Registrierung nicht übertragen werden.

Bei der Initiierung der Domainübertragung müssen Sie sich entweder mit dem Stammkonto oder mit einem Benutzer anmelden, dem auf eine oder mehrere der folgenden Arten IAM-Berechtigungen gewährt wurden:

- Dem Benutzer wird die AdministratorAccessverwaltete Richtlinie zugewiesen.
- Dem Benutzer wird die DomainsFullAccess verwaltete Richtlinie AmazonRoute53 zugewiesen.
- Dem Benutzer wird die FullAccess verwaltete Richtlinie AmazonRoute53 zugewiesen.
- Dem Benutzer wird die PowerUserAccessverwaltete Richtlinie zugewiesen.
- Der Benutzer verfügt über die Berechtigung zum Ausführen aller folgenden Aktionen: `TransferDomains` `DisableDomainTransferLock` und `RetrieveDomainAuthCode`.

Wenn Sie sich weder mit dem Stammkonto noch mit einem Benutzer anmelden, der über die erforderlichen Berechtigungen verfügt, können wir die Übertragung nicht durchführen. Diese Anforderung verhindert, dass nicht autorisierte Benutzer Domänen auf andere übertragen AWS-Konten.

Der Übertragungsvorgang umfasst zwei Schritte: Der ursprüngliche Kontoinhaber startet die Übertragung im Verfahren So übertragen Sie eine Domain an ein anderes AWS-Konto. Danach akzeptiert der Inhaber des Zielkontos die Übertragung im Verfahren So akzeptieren Sie eine Übertragung von einem anderen AWS-Konto.

Um eine Domain auf ein anderes AWS Konto zu übertragen

1. Melden Sie sich mit AWS dem an AWS-Konto , für den die Domain derzeit registriert ist.
2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
4. Wählen Sie den Namen der Domain aus, die Sie an ein anderes AWS-Kontoübertragen möchten.

5. Wählen Sie über dem Abschnitt Details in der Dropdownliste Übertragung aus die Option An ein anderes AWS-Kontoübertragen aus.
6. Geben Sie im Dialogfeld Auf ein anderes AWS-Kontoübertragen die ID des Zielkontos ein. Diese ID erhalten Sie vom Inhaber des AWS-Konto s.
7. Wählen Sie Bestätigen aus.
8. Kopieren Sie im Dialogfeld „Passwort generieren“ das Passwort und leiten Sie es an den empfangenden AWS-Konto Besitzer weiter.

   Auf der Seite Anforderungen wird für die Domain unter Status der Status In Bearbeitung und unter Typ der Wert Interne Übertragung der Domain aus angezeigt.

Um einen Domaintransfer von einem anderen AWS Konto zu akzeptieren

1. Melden Sie sich mit AWS dem an AWS-Konto , der die Domain empfängt.
2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Wählen Sie im Navigationsbereich die Option Anforderungen aus.
4. Wählen Sie auf der Seite Anfragen das Optionsfeld neben dem Domainnamen aus, den Sie von einem anderen übertragen AWS-Konto. Wenn die Domain für die Übertragung bereit ist, hat der Status den Wert Aktion erforderlich und der Typ hat den Wert Interne Übertragung der Domain in.

   Sie haben drei Tage Zeit, um die Anforderung zu akzeptieren. Wenn die Übertragung nicht innerhalb von drei Tagen akzeptiert wurde, wird die Übertragungsanforderung abgebrochen.
5. Wählen Sie in der Dropdownliste Aktion die Option Akzeptieren aus.

   Sie können auch Ablehnen auswählen, um den Übertragungsprozess abzubrechen.
6. Wenn Sie die Übertragung akzeptiert haben, geben Sie auf der Seite Domain auf Ihr Konto übertragen im Bereich Passwort das Passwort ein, das Sie vom ursprünglichen Kontoinhaber erhalten haben.

   Akzeptieren Sie die Bedingungen und wählen Sie Weiter aus.
7. Navigieren Sie zur Seite Anforderungen, um den Übertragungsstatus und weitere auszuführende Schritte zu überprüfen.
8. Nach Abschluss der Übertragung können Sie die Kontaktinformationen aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne.

Programmgesteuertes Übertragen der Domain

Sie können die Domain auch programmgesteuert übertragen, indem Sie die AWS CLI, eine der oder die AWS SDKs Route 53-API verwenden. Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Einen Überblick über den Übertragungsprozess und die Dokumentation zu den API-Aktionen, die Sie verwenden, um eine Domain mithilfe der Route 53-Domain-Registrierungs-API zu übertragen, finden Sie TransferDomainToAnotherAwsAccountin der Amazon Route 53-API-Referenz.
- Eine Dokumentation zu anderen Optionen für die programmgesteuerte Übertragung von Domains finden Sie unter „SDKs & Toolkits“ im Abschnitt Anleitungen und API-Referenzen auf der Seite „AWS Dokumentation“.
- Das Empfängerkonto hat drei Tage Zeit, um die Übertragung vom ursprünglichen Konto mithilfe der -aws-account-API zu akzeptieren. transfer-domain-to-another Wenn die Übertragung nicht innerhalb von drei Tagen akzeptiert wurde, wird die Übertragungsanforderung abgebrochen.

> **Important**
>
> Wenn Sie eine Domain auf ein anderes AWS Konto übertragen, wird die Hosting-Zone für die Domain nicht übertragen. Wenn Sie außerdem die gehostete Zone übertragen möchten, warten Sie, bis die Domäne übertragen wurde. Weitere Informationen finden Sie dann unter Schritt 2 (optional): Migrieren Sie eine gehostete Zone auf ein anderes AWS Konto.

Schritt 2 (optional): Migrieren Sie eine gehostete Zone auf ein anderes AWS Konto

Wenn Sie Route 53 als DNS-Dienst für die Domain verwenden, überträgt Route 53 die gehostete Zone nicht, wenn Sie eine Domain auf ein anderes AWS Konto übertragen. Wenn die Domänenregistrierung einem Konto zugeordnet ist und die entsprechende gehostete Zone mit einem anderen Konto verknüpft ist, ist weder die Domänenregistrierung noch die DNS-Funktionalität betroffen. Der einzige Effekt ist, dass Sie sich bei der Route 53-Konsole mit dem einem Konto anmelden müssen, um die Domäne anzuzeigen, und mit dem anderen Konto für die gehostete Zone.

Wenn Sie das Konto besitzen, von dem Sie die Domäne übertragen, und das Konto, in das Sie die Domäne übertragen, können Sie optional die gehostete Zone für die Domäne in ein anderes

Konto migrieren. Dies ist jedoch nicht erforderlich. Route 53 wird weiterhin die Datensätze in der vorhandenen gehosteten Zone verwenden, um den Datenverkehr für die Domäne zu routen.

> **Important**
>
> Wenn Sie nicht sowohl das Konto besitzen, von dem Sie die Domain übertragen, als auch das Konto, auf das Sie die Domain übertragen, müssen Sie entweder die bestehende Hosting-Zone auf das AWS Konto migrieren, auf das Sie die Domain übertragen, oder eine neue Hosting-Zone in einem AWS Konto erstellen, das Ihnen gehört. Wenn Sie nicht das Konto besitzen, mit dem die gehostete Zone erstellt wurde, die den Datenverkehr für die Domäne leitet, können Sie nicht steuern, wie der Datenverkehr geroutet wird.

Informationen zum Migrieren der vorhandenen gehosteten Zone zum neuen Konto finden Sie unter Migrieren einer Hosting-Zone auf ein anderes Konto AWS.

Informationen zum Erstellen einer neuen gehosteten Zone finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen. Dieses Thema wird normalerweise verwendet, wenn Sie Domains von einem anderen Registrar auf Route 53 übertragen. Der Vorgang ist jedoch derselbe, wenn Sie Domains von einem AWS Konto auf ein anderes übertragen.

> **Important**
>
> White-Label-Nameserver: Wenn Ihre Domain White-Label-Nameserver (benutzerdefinierte Nameserver-Hostnamen wie ns1.example.com) verwendet, sind zusätzliche Schritte erforderlich:
>
> - Bei der Übertragung der Domainregistrierung: Aktualisieren Sie die Glue-Datensätze nach Abschluss der Übertragung bei Ihrem neuen Registrar
> - Bei der Migration von Hosting-Zonen: Aktualisieren Sie die Glue-Einträge nach der Zonenmigration mit Ihrem Domain-Registrar, da sich IP-Adressen ändern, obwohl die Hostnamen gleich bleiben
>
> Detaillierte Anweisungen finden Sie unter the section called “Schritt 7: Erstellen und Ändern der Nameserver der Vergabestelle”.

Anzeigen des Status einer Domänenübertragung

Nachdem Sie die Übertragung einer Domain von einer anderen Domainvergabestelle an Amazon Route 53 gestartet haben, können Sie den Status auf der Seite Anforderungen (neue Konsole) oder auf der Seite Ausstehende Anforderungen (alte Konsole) der Route-53-Konsole nachverfolgen. Die Spalte Status enthält eine kurze Beschreibung des aktuellen Schritts. Die folgende Liste enthält den Text in der Konsole sowie eine detaillierte Beschreibung der einzelnen Schritte.

> **Note**
>
> Wenn Sie eine Übertragungsanfrage einreichen, lautet der anfängliche Status Domain transfer request submitted, der angibt, dass wir Ihre Anforderung erhalten haben.

Ermitteln, ob die Domäne den Übertragungsanforderungen entspricht (Schritt 1 von 14)

Wir bestätigen, dass der Domänenstatus für die Übertragung zulässig ist. Sie müssen Ihre Domäne entsperren, und die Domäne darf keinen der folgenden Statuscodes haben, wenn Sie die Übertragungsanfrage einreichen:

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

TLDs Nur geografisch — Überprüfung der WHOIS-Informationen (Schritt 2 von 14)

Wenn Sie eine Domäne übertragen, die über eine geografische TLD verfügt, haben wir eine WHOIS-Abfrage an Ihre Domäne gesendet, um zu ermitteln, ob Sie den Datenschutz für die Domäne deaktiviert haben. Wenn der Datenschutz bei Ihrer aktuellen Vergabestelle noch aktiviert ist, können wir nicht auf die Informationen zugreifen, die wir benötigen, um die Domäne zu übertragen.

> **Note**
>
> Für Domänen mit einer generischen TLD, wie z. B. .com, .net oder .org, ist keine Autorisierung erforderlich.

TLDs Nur geografisch — E-Mail an den Kontakt des Registranten gesendet, um die Übertragungsautorisierung zu erhalten (Schritt 3 von 14)

Wenn Sie eine Domäne übertragen, die über eine geografische TLD verfügt, haben wir eine E-Mail an den Registranten-Kontakt für die Domäne gesendet. Die E-Mail dient dem Zweck, zu bestätigen, dass die Übertragung von einem autorisierten Kontakt der Domäne angefordert wurde.

> **Note**
>
> Für Domänen mit einer generischen TLD, wie z. B. .com, .net oder .org, ist keine Autorisierung erforderlich.

Überprüfen der Übertragung bei der aktuellen Vergabestelle (Schritt 4 von 14)

Wir haben eine Anforderung an die aktuelle Vergabestelle der Domäne gesendet, um die Übertragung zu initiieren.

TLDs Nur geografisch — Die Genehmigung durch den Ansprechpartner des Registranten steht noch aus (Schritt 5 von 14)

Wir haben eine E-Mail an den Registrierenden für die Domäne gesendet (siehe Schritt 3 von 14) und warten darauf, dass der Registrierende auf einen Link in der E-Mail klickt, um die Übertragung zu autorisieren. Wenn Sie eine Domäne übertragen, die über eine geografische TLD verfügt, und Sie die E-Mail aus irgendeinem Grund nicht erhalten haben, finden Sie weitere Informationen unter Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails.

Kontakt mit aktueller Vergabestelle, um die Übertragung anzufordern (Schritt 6 von 14)

Wir arbeiten mit der aktuellen Vergabestelle zusammen, um die Übertragung der Domäne abzuschließen.

Warten auf die aktuelle Vergabestelle zum Abschluss der Übertragung (Schritt 7 von 14)

Die aktuelle Vergabestelle bestätigt, dass Ihre Domäne die Anforderungen zur Übertragung erfüllt. Dieser Schritt kann bis zu zehn Tagen dauern, abhängig von der TLD für Ihre Domäne:

- Generische Top-Level-Domains – brauchen bis zu sieben Tage
- Geografische Top-Level-Domains (auch als Ländercode-Domänen oberster Ebene bekannt) – brauchen bis zu zehn Tage

> **Note**
>
> Wenn Sie die Bestätigungs-E-Mail genehmigt haben, die bei der Übertragung einer .JP-Domain von Route 53 gesendet wurde, diese jedoch in SCHRITT 7 mehrere Tage lang angehalten wurde, kontaktieren Sie das AWS Supportcenter, wenn Sie Hilfe benötigen.

Im Fall der meisten Vergabestellen ist der Vorgang vollständig automatisiert und kann nicht beschleunigt werden. Einige Vergabestellen senden Ihnen eine E-Mail, in der Sie zur Genehmigung der Übertragung aufgefordert werden. Wenn Ihre Vergabestelle Ihnen diese Bestätigungs-E-Mail sendet, wird der Übertragungsvorgang möglicherweise sehr viel schneller als innerhalb von sieben bis zehn Tagen durchgeführt.

Informationen zu den Gründen, aus denen eine Vergabestelle eine Übertragung möglicherweise ablehnt, finden Sie unter Übertragungsanforderungen für Top-Level-Domains.

Bestätigung durch den Registrierenden, dass der Kontakt die Übertragung initiiert hat (Schritt 8 von 14)

Einige TLD-Registrierungsstellen senden eine weitere E-Mail an den Registrierenden, um zu bestätigen, dass die Übertragung der Domäne von einem autorisierten Benutzer angefordert wurde.

Synchronisieren von Namensservern mit der Registrierungsstelle (Schritt 9 von 14)

Dieser Schritt erfolgt nur dann, wenn die Namensserver, die Sie als Teil der Übertragungsanfrage angegeben haben, sich von den Namensservern unterscheiden, die für die aktuelle Vergabestelle aufgelistet sind. Wir versuchen, Ihre Namensserver auf die neuen Namensserver zu aktualisieren, die Sie angegeben haben.

Synchronisieren der Einstellungen mit der Registrierungsstelle (Schritt 10 von 14)

Wir überprüfen, ob die Übertragung erfolgreich abgeschlossen wurde, und synchronisieren Ihre domänenbezogenen Daten mit unserer Partner-Vergabestelle.

Senden von aktualisierten Kontaktinformationen an die Registrierungsstelle (Schritt 11 von 14)

Wenn Sie den Eigentümer der Domäne bei der Übertragungsanfrage geändert haben, versuchen wir, diese Änderung vorzunehmen. Die meisten Registrierungen ermöglichen jedoch keine Übertragung des Eigentümers als Teil der Domänenübertragung.

Abschließen der Übertragung an Route 53 (Schritt 12 von 14)

Wir bestätigen, dass die Übertragung erfolgreich war.

Abschließen der Übertragung (Schritt 13 von 14)

Wir richten Ihre Domäne in Route 53 ein.

Übertragung abgeschlossen (Schritt 14 von 14)

Die Übertragung wurde erfolgreich abgeschlossen.

Wie sich das Übertragen einer Domain an Amazon Route 53 auf das Ablaufdatum in der Domainregistrierung auswirkt

Wenn Sie eine Domäne zwischen Vergabestellen übertragen, können Sie bei einigen TLD-Registrierungsstellen dasselbe Ablaufdatum für Ihre Domäne beibehalten, einige Registrierungsstellen fügen ein Jahr zum Ablaufdatum hinzu und andere Registrierungsstellen ändern das Ablaufdatum in ein Jahr nach dem Übertragungsdatum.

> **Note**
>
> In den meisten TLDs Fällen können Sie den Registrierungszeitraum für eine Domain um bis zu zehn Jahre verlängern, nachdem Sie sie auf Amazon Route 53 übertragen haben. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

Generisch TLDs

Wenn Sie eine Domäne in Route 53 übertragen, die eine generische TLD hat (z. B. .com), ist das neue Ablaufdatum für die Domäne das Ablaufdatum der vorherigen Vergabestelle plus ein ganzes Jahr.

Geografisch TLDs

Wenn Sie eine Domäne in Route 53 übertragen, die eine geografische TLD hat (z. B. .de), hängt das neue Ablaufdatum für die Domäne von der TLD ab. Suchen Sie Ihre TLD in der folgenden Tabelle, um zu bestimmen, wie die Übertragung der Domäne sich auf das Ablaufdatum auswirkt.

Kontinent	Geografisch TLDs und Auswirkungen der Übertragung einer Domain auf das Ablaufdatum
Afrika	.co.za – Das Ablaufdatum bleibt unverändert.
Nord- und Südamerika	.cl, .com.ar, .com.br – Das Ablaufdatum bleibt unverändert. .ca, .co, .mx, .us – Es wird ein Jahr zum alten Ablaufdatum hinzugefügt.
Asien/Ozeanien	.com.au, .com.sg, .jp, .net.au, .sg — Das Ablaufdatum bleibt gleich. .co.nz, .in, .net.nz, .org.nz — Das alte Ablaufdatum wird um ein Jahr verlängert.
Europa	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se – Das Ablaufdatum bleibt unverändert. .berlin, .eu, .io, .me, .ruhr, .wien – Es wird ein Jahr zum alten Ablaufdatum hinzugefügt. .be, de. .fr, .it, .nl – Das neue Ablaufdatum liegt ein Jahr nach dem Datum der Übertragung.

Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails

Für einige Vorgänge im Zusammenhang mit der Domänenregistrierung verlangt ICANN, dass wir vom Registrierenden für die Domäne autorisiert oder eine Bestätigung erhalten, dass die E-Mail-Adresse des Registrierenden gültig ist. Um die Autorisierung oder Bestätigung zu erhalten, senden wir eine E-Mail mit einem Link. Sie haben je nach Vorgang und Top-Level-Domain zwischen 3 und 15 Tage Zeit, auf den Link zu klicken. Nach dieser Zeit wird der Link funktionsunfähig.

Wenn Sie nicht im vorgesehenen Zeitraum auf den Link in der E-Mail klicken, verlangt ICANN normalerweise, dass wir die Domäne oder den Vorgang stornieren, je nachdem, was Sie tun möchten:

Eine Domain registrieren

Wir unterbrechen die Domäne, damit im Internet nicht darauf zugegriffen werden kann. Um die Bestätigungs-E-Mail erneut zu senden, finden Sie weitere Hinweise unter So senden Sie die Bestätigungs-E-Mail für eine Domänenregistrierung erneut.

TLDs Nur geografisch — Eine Domain zu Amazon Route 53 übertragen

Wenn Sie eine Domäne übertragen, die eine geografische TLD hat, wird die Übertragung von uns abgebrochen. Um die Autorisierungs-E-Mail erneut zu senden, finden Sie weitere Hinweise unter So senden Sie die Autorisierungs-E-Mail für eine Domänenübertragung erneut.

> **Note**
>
> Für Domänen mit einer generischen TLD, wie z. B. .com, .net oder .org, ist keine Autorisierung erforderlich.

Ändern des Namens oder der E-Mail-Adresse des Registrierenden für die Domäne (der Eigentümer)

Wir brechen die Änderung ab. Um die Autorisierungs-E-Mail erneut zu senden, finden Sie weitere Hinweise unter So senden Sie die Autorisierungs-E-Mail zum Aktualisieren des Registrierenden oder zum Löschen der Domäne erneut.

Löschen einer Domain

Wir brechen den Löschvorgang ab. Um die Autorisierungs-E-Mail erneut zu senden, finden Sie weitere Hinweise unter So senden Sie die Autorisierungs-E-Mail zum Aktualisieren des Registrierenden oder zum Löschen der Domäne erneut.

TLDs Nur geografisch — Übertragen Sie eine Domain von Route 53 zu einem anderen Registrar

Wenn Sie eine Domäne übertragen, die eine geografische TLD hat, wird die Übertragung von der neuen Vergabestelle abgebrochen.

> **Note**
>
> Für Domänen mit einer generischen TLD, wie z. B. .com, .net oder .org, ist keine Autorisierung erforderlich.

Themen

Aktualisieren Ihrer E-Mail-Adresse

Wir senden immer Bestätigungs-E-Mails und Autorisierungs-E-Mails an die Adresse des Registrierenden für eine Domäne. In einigen TLDs Fällen müssen wir in den folgenden Fällen E-Mails an die alten und neuen E-Mail-Adressen der Kontaktperson des Registranten senden:

- Sie ändern die E-Mail-Adresse für eine Domain, die bereits bei Amazon Route 53 registriert ist
- Sie ändern die E-Mail-Adresse für eine Domain, die Sie an Route 53 übertragen

Erneutes Senden von E-Mails

Verwenden Sie die entsprechenden Verfahren zum erneuten Senden von Bestätigungs- oder Autorisierung-E-Mails.

- So senden Sie die Bestätigungs-E-Mail für eine Domänenregistrierung erneut
- So senden Sie die Autorisierungs-E-Mail für eine Domänenübertragung erneut
- So senden Sie die Autorisierungs-E-Mail zum Aktualisieren des Registrierenden oder zum Löschen der Domäne erneut

So senden Sie die Bestätigungs-E-Mail für eine Domänenregistrierung erneut

1. Überprüfen Sie die E-Mail-Adresse für den Registrierenden und aktualisieren Sie sie bei Bedarf. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne.
2. Überprüfen Sie den Spam-Ordner in Ihrer E-Mail-Anwendung auf eine E-Mail von einer der folgenden E-Mail-Adressen.

   Wenn zu viel Zeit vergangen ist, funktioniert der Link nicht mehr, aber Sie wissen, wo sich die Bestätigungs-E-Mail befindet, wenn wir Ihnen einen anderen Link schicken.

TLDs	E-Mail-Adresse, von der die Genehmigungs- oder Bestätigungs-E-Mail kommt

TLDs	E-Mail-Adresse, von der die Genehmigungs- oder Bestätigungs-E-Mail kommt
.fr	nic@nic.fr
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> Die E-Mails enthalten möglicherweise einen Link zu „www.verify-whois.com“. Dieser Link ist sicher.

3. Verwenden Sie die Amazon Route 53-Konsole zum erneuten Senden der Bestätigungs-E-Mail:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   b. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).

   c. Wählen Sie den Namen der Domäne aus, für die erneut eine E-Mail gesendet werden soll.

   d. Klicken Sie in der Warnmeldung mit der Überschrift "Your domain might be suspended" auf Send email again.

   > **Note**
   >
   > Wenn es keine Warnmeldung gibt, haben Sie bereits bestätigt, dass die E-Mail-Adresse für den Registrierenden gültig ist.

4. Wenn Sie beim erneuten Senden der Bestätigungs-E-Mail auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

So senden Sie die Autorisierungs-E-Mail für eine Domänenübertragung erneut

Diese Methode funktioniert nicht für .jp Domain-Transferanforderungen.

1. Verwenden Sie die Methode, die von der aktuellen Vergabestelle für die Domäne angegeben ist, um zu bestätigen, dass der Datenschutz für die Domäne deaktiviert ist. Falls nicht, deaktivieren Sie ihn.

   Wir senden die Autorisierungs-E-Mail an die E-Mail-Adresse, die die aktuelle Vergabestelle in der WHOIS-Datenbank gespeichert hat. Wenn Datenschutz aktiviert ist, wird die E-Mail-Adresse in der Regel verschleiert. Die aktuelle Vergabestelle leitet die E-Mail, die Amazon Route 53 an die E-Mail-Adresse in der WHOIS-Datenbank gesendet hat, möglicherweise nicht an Ihre tatsächliche E-Mail-Adresse weiter.

   > **Note**
   >
   > Wenn die aktuelle Vergabestelle für die Domäne Sie den Datenschutz nicht abschalten lässt, können wir die Domäne trotzdem übertragen, wenn Sie in Schritt 5: Anfordern der Übertragung einen gültigen Autorisierungscodeangegeben haben.

2. Überprüfen Sie die E-Mail-Adresse für den Registrierenden und aktualisieren Sie sie bei Bedarf. Verwenden Sie die Methode, die von der aktuellen Vergabestelle für die Domäne angegeben ist.
3. Überprüfen Sie den Spam-Ordner in Ihrer E-Mail-Anwendung auf eine E-Mail von einer der folgenden E-Mail-Adressen.

   Wenn zu viel Zeit vergangen ist, funktioniert der Link nicht mehr, aber Sie wissen, wo sich die Autorisierungs-E-Mail befindet, wenn wir Ihnen einen anderen Link schicken.

TLDs	E-Mail-Adresse, von der die Genehmigungs- oder Bestätigungs-E-Mail kommt
.com.au und .net.au	no-reply@ispapi.net

TLDs	E-Mail-Adresse, von der die Genehmigungs- oder Bestätigungs-E-Mail kommt
	Die E-Mail enthält einen Link zuhttps://approve.domainadmin.com.
.fr	nic@nic.fr
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon • noreply@domainnameverification.net • noreply@emailverification.info

> **Note**
>
> Die E-Mails enthalten möglicherweise einen Link zu „www.verify-whois.com“. Dieser Link ist sicher.

4. Wenn die Übertragung nicht mehr läuft (da wir den Prozess bereits abgebrochen haben, wenn zu viel Zeit vergangen ist), fordern Sie die Übertragung erneut an. Wir senden Ihnen dann erneut eine Autorisierungs-E-Mail zu.

> **Note**
>
> Für die ersten 15 Tage nach der Anforderung der Übertragung können Sie den Status der Übertragung bestimmen, indem Sie die TabelleNotifications (Benachrichtigungen) auf der Seite Dashboard in der Route 53-Konsole aufrufen. Verwenden Sie nach 15 Tagen den, AWS CLI um den Status abzurufen. Weitere Informationen finden Sie unter route53domains im AWS CLI Command Reference.

Wenn die Übertragung noch nicht abgeschlossen ist, führen Sie die folgenden Schritte aus, um die Autorisierungs-E-Mail erneut zu senden.

a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

b. Suchen Sie in der Tabelle Alerts die Domäne, die Sie übertragen möchten.

c. Klicken Sie in der Spalte Status für diese Domäne auf E-Mail erneut senden.

5. Wenn Sie beim erneuten Senden der Autorisierungs-E-Mail für einen Domaintransfer auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

So senden Sie die Autorisierungs-E-Mail zum Aktualisieren des Registrierenden oder zum Löschen der Domäne erneut

1. Überprüfen Sie die E-Mail-Adresse für den Registrierenden und aktualisieren Sie sie bei Bedarf. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne.
2. Überprüfen Sie den Spam-Ordner in Ihrer E-Mail-Anwendung auf eine E-Mail von einer der folgenden E-Mail-Adressen.

   Wenn zu viel Zeit vergangen ist, funktioniert der Link nicht mehr, aber Sie wissen, wo sich die Autorisierungs-E-Mail befindet, wenn wir Ihnen einen anderen Link schicken.

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt
.fr	nic@nic.fr
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon • noreply@domainnameverification.net

TLDs	E-Mail-Adresse, von der die Autorisierungs-E-Mail kommt
	• noreply@emailverification.info

> **Note**
>
> Die E-Mails enthalten möglicherweise einen Link zu „www.verify-whois.com“. Dieser Link ist sicher.

3. Abbrechen der Änderung oder der Löschung. Sie haben zwei Optionen:

   - Sie können die 3 bis 15 Tage abwarten, nach dem wir automatisch den angeforderten Vorgang abbrechen.
   - Alternativ können Sie sich an den AWS Support wenden und ihn bitten, den Vorgang abzubrechen.

> **Important**
>
> Transferarten und Stornierungsmethoden: Die Stornierungsmethode hängt von der Art der Überweisung ab:
>
> - Externer Registrar für Route 53: Folgen Sie den Anweisungen in diesem Thema (warten Sie auf die automatische Stornierung oder wenden AWS Sie sich an den Support)
> - Zwischen AWS Konten: Verwenden Sie die `CancelDomainTransferToAnotherAwsAccount` API oder wenden Sie sich an den AWS Support
>
> Wenden Sie sich nicht an Ihren aktuellen externen Registrar, um eine Übertragung zu Route 53 zu stornieren, da er Übertragungen, die bereits im Gange sind, nicht stornieren kann. AWS

4. Nachdem die Änderung oder der Löschvorgang storniert wurde, können Sie die Kontaktinformationen ändern oder die Domäne erneut löschen, und wir senden Ihnen eine weitere Autorisierungs-E-Mail.
5. Wenn Sie beim erneuten Senden der Autorisierungs-E-Mail auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Konfigurieren von DNSSEC für eine Domäne

Angreifer fangen manchmal Datenverkehr an Internetendpunkte wie Webserver ab, indem sie DNS-Abfragen abfangen und ihre eigenen IP-Adressen anstelle der tatsächlichen IP-Adressen für diese Endpunkte an die DNS-Auflöser zurückgeben. Die Benutzer werden dann in die IP-Adressen aus der gefälschten Antwort der Angreifer geleitet, z. B. auf gefälschte Websites.

Sie können Ihre Domain vor dieser Art von Angriff schützen, die als DNS-Spoofing oder man-in-the-middle Angriff bezeichnet wird, indem Sie Domain Name System Security Extensions (DNSSEC), ein Protokoll zur Sicherung des DNS-Verkehrs, konfigurieren.

> **Important**
>
> Amazon Route 53 unterstützt die DNSSEC-Signierung sowie DNSSEC für die Domainregistrierung. Informationen zum Konfigurieren der DNSSEC-Signierung für eine Domäne, die in Route 53 registriert ist, finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

Themen

- Übersicht über den Schutz Ihrer Domäne durch DNSSEC
- Voraussetzungen und Höchstwerte für die Konfiguration von DNSSEC für eine Domäne
- Hinzufügen von öffentlichen Schlüsseln für eine Domäne
- Löschen von öffentlichen Schlüsseln für eine Domäne

Übersicht über den Schutz Ihrer Domäne durch DNSSEC

Wenn Sie DNSSEC für Ihre Domäne konfigurieren, erstellt ein DNS-Auflöser eine Vertrauenskette für Antworten von zwischengeschalteten Auflösern. Die Vertrauenskette beginnt mit der TLD-

Registrierungsstelle für die Domäne (die übergeordnete Zone der Domäne) und endet mit den autoritativen Namensservern bei Ihrem DNS-Dienstanbieter. Nicht alle DNS-Auflöser unterstützen DNSSEC. Nur Resolver, die DNSSEC unterstützen, führen eine Signatur- oder Authentizitätsüberprüfung durch.

So konfigurieren Sie DNSSEC für Domänen, die mit Amazon Route 53 registriert sind, um Ihre Internet-Hosts vor DNS-Spoofing zu schützen (vereinfacht zur besseren Darstellung):

1. Verwenden Sie die Methode Ihres DNS-Dienstanbieter zum Signieren von Datensätzen in Ihrer gehosteten Zone mit dem privaten Schlüssel in einem asymmetrischen Schlüsselpaar.

   > **Important**
   >
   > Route 53 unterstützt die DNSSEC-Signierung sowie DNSSEC für die Domainregistrierung. Weitere Informationen hierzu finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

2. Geben Sie den öffentlichen Schlüssel des Schlüsselpaares an die Domänenvergabestelle weiter, und geben Sie den Algorithmus an, der verwendet wurde, um das Schlüsselpaar zu generieren. Die Domänenvergabestelle leitet den öffentlichen Schlüssel und den Algorithmus zur Registrierungsstelle für die Top-Level-Domain (TLD) weiter.

   Weitere Informationen darüber, wie Sie diesen Schritt für Domänen ausführen, die Sie mit Route 53 registriert haben, finden Sie unter Hinzufügen von öffentlichen Schlüsseln für eine Domäne.

Nach der Konfiguration von DNSSEC wird Ihre Domäne wie folgt vor DNS-Spoofing geschützt:

1. Senden Sie eine DNS-Abfrage, zum Beispiel, indem Sie auf einer Website surfen oder durch Senden einer E-Mail-Nachricht.
2. Die Anforderung wird an den DNS-Auflöser weitergeleitet. Auflöser sind zuständig für die Rückgabe des entsprechenden Werts an Kunden basierend auf der Anforderung, z. B. die IP-Adresse für den Host, auf dem ein Webserver oder ein E-Mail-Server ausgeführt wird.
3. Wenn die IP-Adresse im DNS-Resolver zwischengespeichert ist, da jemand anders bereits die gleiche DNS-Abfrage übermittelt hat und der Resolver bereits über den Wert verfügt, gibt der Resolver die IP-Adresse an den Client zurück, der die Anforderung übermittelt hat. Der Client verwendet dann die IP-Adresse für den Zugriff auf den Host.

Wenn die IP-Adresse nicht im DNS-Auflöser zwischengespeichert ist, sendet der Auflöser eine Anforderung an die übergeordnete Zone für Ihre Domäne in der TLD-Registrierungsstelle, die daraufhin zwei Werte zurückgibt:

- Der Delegation Signer (DS)-Datensatz, bei dem es sich um einen öffentlichen Schlüssel handelt, der dem privaten Schlüssel entspricht, welcher zum Signieren des Datensatzes verwendet wurde.
- Die IP-Adressen der autoritativen Namenserver für die Domäne.

4. Der DNS-Auflöser sendet die ursprüngliche Anforderung an einen anderen DNS-Auflöser. Wenn dieser Auflöser nicht über die IP-Adresse verfügt, wiederholt er den Prozess, bis ein Auflösungsdienst die Anforderung an einen Namensserver bei Ihrem DNS-Dienstanbieter sendet. Der Namenserver gibt zwei Werte zurück:
   - Den Datensatz für die Domäne, wie z. B. example.com. Im Allgemeinen enthält dieser die IP-Adresse eines Hosts.
   - Die Signatur für den Datensatz, den Sie bei der Konfiguration von DNSSEC erstellt haben.
5. Der DNS-Resolver verwendet den öffentlichen Schlüssel, den Sie der Domainvergabestelle mitgeteilt haben und der von der Vergabestelle an die TLD-Registrierungsstelle weitergeleitet wurde, um die beiden folgenden Dinge auszuführen:
   - Erstellen einer Vertrauenskette.
   - Überprüfen Sie, ob die signierte Antwort vom DNS-Dienstanbieter rechtmäßig ist und nicht durch eine schädliche Antwort von einem Angreifer ersetzt wurde.
6. Wenn die Antwort authentisch ist, gibt der Auflöser den Wert an den Client zurück, der die Anforderung übermittelt hat.

   Wenn die Antwort nicht verifiziert werden kann, wird vom Auflöser ein Fehler an den Benutzer zurückgegeben.

   Wenn die TLD-Registrierungsstelle für die Domäne nicht über den öffentlichen Schlüssel der Domäne verfügt, beantwortet der Auflöser die DNS-Abfrage mit der Antwort, die er vom DNS-Dienstanbieter erhalten hat.

Voraussetzungen und Höchstwerte für die Konfiguration von DNSSEC für eine Domäne

Um DNSSEC für eine Domäne zu konfigurieren, müssen Ihre Domäne und Ihr DNS-Dienstanbieter die folgenden Voraussetzungen erfüllen:

- Die Registrierungsstelle für die TLD muss DNSSEC unterstützen. Informationen darüber, wie Sie bestimmen, ob die Registrierung für Ihre TLD DNSSEC unterstützt, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.
- Der DNS-Dienstanbieter für die Domäne müssen DNSSEC unterstützen.

> **Important**
>
> Route 53 unterstützt die DNSSEC-Signierung sowie DNSSEC für die Domainregistrierung. Weitere Informationen hierzu finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

- Sie müssen DNSSEC mit dem DNS-Service-Anbieter für Ihre Domäne konfigurieren, bevor Sie öffentliche Schlüssel für die Domäne in Route 53 hinzufügen können.
- Die Anzahl der öffentlichen Schlüssel, die Sie zu einer Domäne hinzufügen können, hängt von der TLD für die Domäne ab:
  - .com- und .net-Domänen – bis zu dreizehn Schlüssel
  - Alle anderen Domänen – bis zu vier Schlüssel

Hinzufügen von öffentlichen Schlüsseln für eine Domäne

Wenn Sie die Schlüssel wechseln oder wenn Sie DNSSEC für eine Domäne aktivieren, führen Sie die folgenden Schritte durch, nachdem Sie DNSSEC mit dem DNS-Dienstanbieter für die Domäne konfiguriert haben.

So fügen Sie öffentliche Schlüssel für eine Domäne hinzu

1. Wenn Sie nicht bereits DNSSEC für Ihren DNS-Dienstanbieter konfiguriert haben, verwenden Sie die von Ihrem Service-Anbieter bereitgestellte Methode zur Konfiguration von DNSSEC.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/

3. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domänen).
4. Klicken Sie auf den Namen der Domäne, für die Sie Schlüssel hinzufügen möchten.
5. Wählen Sie auf dem Tab DNSSEC-Schlüssel die Option Schlüssel hinzufügen aus.
6. Geben Sie die folgenden Werte an:

   Schlüsseltyp

   Wählen Sie, ob Sie einen Schlüssel-Signaturschlüssel (KSK) oder einen Zonen-Signaturschlüssel (ZSK) hochladen möchten.

   Algorithmus

   Wählen Sie den Algorithmus, den Sie zum Signieren der Datensätze für die gehostete Zone verwendet haben.

   Öffentlicher Schlüssel

   Geben Sie den öffentlichen Schlüssel des asymmetrischen Schlüsselpaars an, den Sie für die Konfiguration von DNSSEC für Ihrem DNS-Dienstanbieter verwendet haben.

   Beachten Sie Folgendes:

   - Geben Sie den öffentlichen Schlüssel an, nicht den Digest.
   - Sie müssen den Schlüssel im base64-Format angeben.
7. Wählen Sie Hinzufügen aus.

   > **Note**
   >
   > Sie können nur jeweils einen öffentlichen Schlüssel hinzufügen. Wenn Sie weitere Schlüssel hinzufügen möchten, warten Sie, bis Sie eine Bestätigungs-E-Mail von Route 53 erhalten haben.
8. Wenn Route 53 eine Antwort von der Registrierungsstelle erhält, senden wir eine E-Mail an den Registrierenden für die Domäne. Die E-Mail bestätigt entweder, dass der öffentliche Schlüssel in der Registrierungsstelle zur Domäne hinzugefügt wurde oder erklärt, warum der Schlüssel nicht hinzugefügt werden konnte.

Löschen von öffentlichen Schlüsseln für eine Domäne

Wenn Sie die Schlüssel wechseln oder wenn Sie DNSSEC für eine Domäne deaktivieren, löschen Sie die öffentlichen Schlüssel mit den folgenden Schritten, bevor Sie DNSSEC bei Ihrem DNS-Dienstanbieter deaktivieren. Beachten Sie Folgendes:

- Wenn Sie die öffentlichen Schlüssel wechseln, empfehlen wir, dass Sie bis zu drei Tage warten, nachdem Sie die neuen öffentlichen Schlüssel hinzugefügt haben, bevor Sie die alten öffentlichen Schlüssel löschen.
- Wenn Sie DNSSEC deaktivieren, löschen Sie zuerst die öffentlichen Schlüssel für die Domäne. Wir empfehlen, dass Sie bis zu drei Tage warten, bevor Sie DNSSEC beim DNS-Dienst für die Domäne deaktivieren.

> **Important**
>
> Wenn DNSSEC für die Domäne aktiviert ist und Sie DNSSEC beim DNS-Dienst deaktivieren, geben DNS-Auflöser, die DNSSEC unterstützen, einen `SERVFAIL`-Fehler an Clients zurück, und Clients haben keinen Zugriff mehr auf die Endpunkte, die mit der Domäne verknüpft sind.

So löschen Sie öffentliche Schlüssel für eine Domäne

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domänen).
3. Klicken Sie auf den Namen der Domäne, in der Sie Schlüssel löschen möchten.
4. Aktivieren Sie auf dem Tab DNSSEC-Schlüssel das Optionsfeld neben dem Schlüssel, den Sie löschen möchten, und anschließend Schlüssel löschen aus.
5. Geben Sie im Dialogfeld DNSSEC-Schlüssel löschen den Text Löschen in das Textfeld ein, um zu bestätigen, dass Sie den Schlüssel löschen möchten, und wählen Sie dann Löschen aus.

   > **Note**
   >
   > Sie können nur jeweils einen öffentlichen Schlüssel löschen. Wenn Sie weitere Schlüssel löschen möchten, warten Sie, bis Sie eine Bestätigungs-E-Mail von Amazon Route 53 erhalten haben.

6. Wenn Route 53 eine Antwort von der Registrierungsstelle erhält, senden wir eine E-Mail an den Registrierenden für die Domäne. Die E-Mail bestätigt entweder, dass der öffentliche Schlüssel in der Registrierungsstelle aus der Domäne gelöscht wurde oder erklärt, warum der Schlüssel nicht gelöscht werden konnte.

Ihre Vergabestelle und andere Informationen zu Ihrer Domain finden

Um Domäneninformationen mithilfe der GetDomainDetailAPI anzuzeigen, können Sie eine der Optionen SDKs oder verwenden AWS CLI. Weitere Informationen finden Sie unter get-domain-detail.

Informationen über Domains mit **`get-domain-detail`** CLI anzeigen

- Verwenden Sie die folgende CLI:

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> Dieser Befehl läuft nur in us-east-1 AWS-Region.

Alle Informationen zu Ihrer Domain werden in der Ausgabe aufgeführt, einschließlich Vergabestelle, Registrierungsdatum, Datenschutzeinstellung usw.

Anzeigen von Informationen zu Domains, die bei Route 53 registriert sind

> **Note**
>
> Ab dem 28. Januar 2025 können einige Domain-Registries für Abfragen von Domainregistrierungsdaten von WHOIS auf das Registration Data Access Protocol (RDAP) umsteigen. Wenn Sie über WHOIS direkt von Registern aus auf Informationen zur Domainregistrierung zugreifen, müssen Sie Ihre Anwendungen möglicherweise aktualisieren,

sodass sie RDAP-Endpunkte verwenden, falls die entsprechende Registry die WHOIS-Unterstützung einstellt.
Die Funktionalität des Route 53-Domains-Dienstes bleibt unverändert. Dieser Hinweis gilt nur für direkte WHOIS-Abfragen in der Registrierung, die außerhalb der Route 53-Dienste durchgeführt werden.

Sie können Informationen zu Domains anzeigen, die unter Verwendung von Route 53 registriert wurden. Zu diesen Informationen gehören Angaben wie das Datum, an dem die Domain ursprünglich registriert wurde, und Kontaktinformationen für den Domaininhaber sowie für die Ansprechpartner für Technik, Verwaltung und Rechnungsstellung.

WHOIS

WHOIS ist ein kostenloses, öffentlich zugängliches Verzeichnis mit Informationen zu Domains, die von Domainvergabestellen und Registrierungsstellen gesponsert werden. Es wird sowohl als Dienst bereitgestellt, der Anfragen über Port 43 akzeptiert, als auch als Website, auf die jeweils IPv4 sowohl als auch zugegriffen werden kann IPv6. WHOIS ist eine verteilte hierarchische Suche. Weitere Informationen zu WHOIS finden Sie hier.

Eine WHOIS-Anforderung an verschiedene Hierarchieebenen kann unterschiedliche Informationen liefern:

- Eine WHOIS-Anforderung auf Stammebene (whois.iana.org) liefert Informationen zur Registrierungsstelle.
- Eine WHOIS-Anforderung auf Registrierungsstellenebene liefert Informationen zur Vergabestelle sowie einige öffentliche Informationen zur Domain.
- Eine WHOIS-Anforderung auf Vergabestellenebene liefert alle öffentlichen Informationen zur Domain.

Da es mehrere Ebenen von WHOIS gibt (einschließlich WHOIS-Suchvorgänge, die von der TLD-Registrierungsstelle und der Domain-Vergabestelle durchgeführt werden), kann es sein, dass die Deaktivierung Ihres Datenschutzes in der Route-53-Konsole nur für WHOIS auf Vergabestellenebene wirksam ist. Einige Registrierungsstellen behalten bewusst Datenschutz- oder Unkenntlichmachungsservices für ihre WHOIS-Suchservices bei, und zwar unabhängig davon, ob Sie sie mit Route 53 deaktiviert haben. Um vollständige Informationen zu Ihrer Domain zu erhalten, empfehlen wir, die von der Vergabestelle bereitgestellte WHOIS-Suche zu verwenden.

Beachten Sie Folgendes:

Senden von Domainkontakten bei aktiviertem Datenschutz

Wenn der Datenschutz für die Domain aktiviert ist, werden Kontaktinformationen für den Registrierenden sowie technische und administrative Kontakte durch Kontaktinformationen für den Amazon Registrar-Datenschutz ersetzt. Ein Beispiel: Wenn die Domain „example.com“ bei Amazon Registrar registriert und der Datenschutz aktiviert ist, sieht der Wert von E-Mail-Adresse des Registranten in der Antwort auf eine WHOIS-Abfrage in etwa wie folgt aus: besitzer1234@example.com.identity-protect.org.

Um bei aktiviertem Datenschutz mindestens einen Domainkontakt zu kontaktieren, senden Sie eine E-Mail an die entsprechenden E-Mail-Adressen. Wir leiten Ihre E-Mail automatisch an den entsprechenden Ansprechpartner weiter.

Missbrauch melden

Um illegale Aktivitäten oder Verstöße gegen die Nutzungsbedingungen, einschließlich unangemessener Inhalte, Phishing, Malware oder Spam, zu melden, senden Sie eine E-Mail an trustandsafety@support.aws.com.

So zeigen Sie Informationen zu Domains an, die bei Route 53 registriert sind

1. Navigieren Sie in einem Webbrowser zu einer der folgenden Websites:
   - Amazon-Registrar WHOIS: /whois https://registrar.amazon.com
   - Amazon-Registrar RDAP: /rdap https://registrar.amazon.com
   - Gandi WHOIS: https://whois.gandi.net
2. Geben Sie den Namen der Domain ein, zu der Sie Informationen anzeigen möchten, und wählen Sie Search (Suchen) aus.

Löschen einer Domainnamen-Registrierung

Bei den meisten Top-Level-Domains (TLDs) können Sie die Registrierung löschen, wenn Sie sie nicht mehr benötigen. Wenn die Registrierungsstelle das Löschen der Registrierung zulässt, führen Sie die Schritte in diesem Thema aus.

Beachten Sie Folgendes:

Die Registrierungsgebühr kann nicht zurückerstattet werden

Wenn Sie eine Domainnamen-Registrierung löschen, bevor die Registrierung abläuft, erstattet AWS die Registrierungsgebühr nicht.

TLDs die es Ihnen ermöglichen, eine Domainregistrierung zu löschen

Informationen dazu, ob Sie die Registrierung für Ihre Domain löschen können, finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können. Wenn der Abschnitt für Ihre TLD keinen Unterabschnitt "Löschen der Domainregistrierung" enthält, können Sie die Domain löschen. Bevor Sie die Domain löschen, stellen Sie sicher, dass Sie die Domainsperre deaktiviert haben. Weitere Informationen zur Deaktivierung der Domainsperre finden Sie unter DisableDomainTransferLock.

Was geschieht, wenn Sie eine Domainregistrierung nicht löschen können?

Wenn die Registry für Ihre Domain das Löschen der Domainnamen-Registrierung nicht zulässt, müssen Sie warten, bis die Domain abläuft. Um sicherzustellen, dass die Domain nicht automatisch erneuert wird, deaktivieren Sie die automatische Erneuerung für die Domain. Sobald das Ablaufdatum unter Expires on (Läuft ab am) erreicht ist, löscht Route 53 die Registrierung für die Domain automatisch. Weitere Informationen zum Ändern der automatischen Verlängerungseinstellung finden Sie unter Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne.

Verzögerung, bevor eine Domain gelöscht wird und zur erneuten Registrierung wieder verfügbar ist

Nahezu alle Registries verhindern alle Benutzer, sofort eine Domain zu registrieren, die gerade abgelaufen ist. Die typische Verzögerung beträgt je nach TLD ein bis drei Monate. Weitere Informationen finden Sie im Abschnitt "Fristen für die Verlängerung und Wiederherstellung von Domains" für Ihre TLD in Domains, die Sie mit Amazon Route 53 registrieren können.

> **Important**
>
> Löschen Sie eine Domain nicht und rechnen Sie damit, sie erneut zu registrieren, wenn Sie die Domain nur zwischen AWS Konten übertragen oder die Domain an einen anderen Registrar übertragen möchten. Siehe stattdessen in der entsprechenden Dokumentation:
>
> - Übertragung einer Domain auf ein anderes AWS Konto
> - Überträgt eine Domain von Amazon Route 53 zu einer anderen Vergabestelle.

So löschen Sie eine Domainnamen-Registrierung

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domains).
3. Wählen Sie den Namen der Domain aus.

   Informationen zum Löschen einer .co.uk-, .me.uk-, .org.uk- oder .uk-Domain finden Sie unter Um Domainnamen-Registrierungen der Domainnamen .co.uk, .me.uk, .org.uk und .uk zu löschen.
4. Wenn die Registrierungsstelle für Ihre TLD das Löschen einer Domainnamenregistrierung zulässt, wählen Sie Domain löschen aus.

   Bei einigen Domains muss von uns eine E-Mail an den Registranten der Domain gesendet werden, um sicherzustellen, dass der Registrant die Domain löschen möchte. Wenn Sie eine E-Mail erhalten, stammt sie von einer der folgenden E-Mail-Adressen:

   - noreply@registrar.amazon — für die TLDs Registrierung bei Amazon Registrar.
   - noreply@domainnameverification.net oder noreply@emailverification.info — für die TLDs Registrierung durch unseren Registrar-Mitarbeiter Gandi.

   Die zuständige Vergabestelle für Ihre TLD finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.
5. Wenn Sie die Verifizierungs-E-Mail erhalten, wählen Sie den Link in der E-Mail aus und genehmigen Sie die Anforderung zum Löschen der Domain oder lehnen Sie sie ab.

   > **Important**
   >
   > Der Ansprechpartner des Registranten muss sofort den Anweisungen in der E-Mail folgen, oder wir müssen den Löschantrag nach Ablauf eines Tages stornieren, wie es von ICANN verlangt wird.

   Sie erhalten eine weitere E-Mail, sobald Ihre Domain gelöscht wurde. Informationen zum Verfolgen des aktuellen Status Ihrer Anforderungen finden Sie unter Anzeigen des Status einer Domainregistrierung.
6. Löschen Sie erst die Datensätze in der gehosteten Zone für die gelöschte Domain und dann die gehostete Zone. Nachdem Sie die gehostete Zone gelöscht haben, wird Ihnen die monatliche

Gebühr für die gehostete Zone von Route 53 nicht mehr in Rechnung gestellt. Weitere Informationen finden Sie in der folgenden Dokumentation:

- Löschen von Datensätzen
- Löschen einer öffentlichen gehosteten Zone
- Route-53-Preise

7. Wenn Sie beim Löschen einer Domainnamenregistrierung auf Probleme stoßen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Um Domainnamen-Registrierungen der Domainnamen .co.uk, .me.uk, .org.uk und .uk zu löschen

Wenn Sie eine.uk-, .me.uk-, .org.uk- oder .uk-Domain löschen möchten, erstellen Sie ein Konto bei Nominet, der Registry für.uk-Domains. Weitere Informationen finden Sie unter "Cancelling your domain name" auf der Nominet-Website, https://www.nominet.uk/domain-support/.

> **Important**
>
> Wenn Sie einen.uk-Domainnamen löschen (kündigen), wird er innerhalb weniger Tage gelöscht und kann von jedem registriert werden. Wenn Sie die Domain nur übertragen möchten, löschen Sie sie nicht.

Es folgt eine Übersicht über den Prozess:

1. Befolgen Sie auf der Nominet-Website die Anleitung zur erstmaligen Anmeldung. Siehe https://secure.nominet.org.uk/auth/login.html. Nominet sendet Ihnen eine E-Mail mit Anweisungen zum Erstellen eines Passworts.
2. Folgen Sie den Anweisungen in der E-Mail, die Sie von Nominet erhalten.
3. Melden Sie sich bei der Nominet-Website an und folgen Sie den Anweisungen zum Abbrechen (Löschen) eines Domainnamens.

Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support

AWS bietet einen kostenlosen Basis-Supportplan für alle AWS Kunden. Der Plan umfasst die Unterstützung bei folgenden Problemen im Zusammenhang mit der Domainregistrierung:

- Übertragen von Domains von oder zu Amazon Route 53
- Übertragung von Domains zwischen AWS Konten
- Erhöhen der Kontingente für Route-53-Entitäten, wie z. B. die Anzahl der Domains, die Sie registrieren können (weitere Informationen unter Kontingente.)
- Ändern des Besitzers einer Domain
- Ändern der Kontaktinformationen für den Eigentümer einer Domain
- Erneutes Senden von Bestätigungs- und Autorisierungs-Emails
- Erneuern von Domains
- Wiederherstellen von abgelaufenen Domains
- Abrufen von Route 53-Rechnungsinformationen
- Bereitstellen von Identitätsnachweisen für .uk-Domains
- Löschen von Domains oder Deaktivierung der automatischen Verlängerung nach dem Schließen Ihres Kontos AWS

Um den AWS Support zu diesen und anderen Problemen im Zusammenhang mit der Domainregistrierung zu kontaktieren, führen Sie das entsprechende Verfahren durch.

Themen

Wenden Sie sich an den AWS Support, wenn Sie sich bei Ihrem AWS Konto anmelden können

Gehen Sie wie folgt vor, um den AWS Support zu kontaktieren, wenn Sie sich AWS bei Ihrem Konto anmelden können:

1. Melden Sie sich mit dem AWS Konto, für das die Domain derzeit registriert ist, beim AWS Support an.

   > **Important**
   >
   > Sie müssen sich mit dem Stammkonto anmelden, unter dem die Domain derzeit registriert ist. Diese Anforderung verhindert, dass nicht autorisierte Benutzer Ihr Konto entführen.

2. Wählen Sie Konto und Abrechnung
3. Geben Sie die folgenden Werte an:

   Regarding

   Übernehmen Sie den Standardwert für Account and Billing Support.

   Service

   Akzeptieren Sie den Standardwert von Domains.

   Kategorie

   Akzeptieren Sie den Standardwert für Registration Issue.

   Schweregrad

   Wählen Sie den zutreffenden Schweregrad.

   Betreff

   Geben Sie eine kurze Zusammenfassung des Problems ein.

   Description

   Beschreiben Sie das Problem genauer und fügen Sie relevante Dokumente oder Screenshots bei.

   Kontaktmethode

   Wählen Sie die Kontaktmethode Web aus. Wir werden Sie über die E-Mail-Adresse kontaktieren, die mit Ihrem AWS Konto verknüpft ist.

4. Wählen Sie Absenden aus.

AWS Support kontaktieren, wenn Sie sich nicht bei Ihrem AWS Konto anmelden können

Gehen Sie wie folgt vor, um den AWS Support zu kontaktieren, wenn Sie sich nicht AWS bei Ihrem Konto anmelden können:

1. Gehen Sie zur Support-Seite Ich bin AWS Kunde und suche nach Abrechnungs- oder Kontounterstützung.
2. Füllen Sie das Formular aus.
3. Wählen Sie Absenden aus.

Herunterladen von Domains-Rechnungsberichten

Wenn Sie mehrere Domains verwalten und die Kosten nach Domain für einen bestimmten Zeitraum anzeigen möchten, können Sie einen Domains-Rechnungsbericht herunterladen. Dieser Bericht enthält alle Gebühren für die Domainregistrierung, einschließlich der folgenden:

- Registrieren einer Domain
- Verlängern der Registrierung für eine Domain
- Übertragen meiner Domain an Amazon Route 53
- Den Besitzer einer Domain ändern (für einige TLDs ist dieser Vorgang kostenlos)

Manchmal kann Ihr Abrechnungsbericht Abrechnungszeiträume in der Zukunft anzeigen. Dies liegt daran, dass der Prozess der automatischen Verlängerung der Domain im Monat vor Ablauf der Domain beginnt. Daher wird in Ihrem August-Bericht möglicherweise ein Abrechnungszeitraum angezeigt, der im darauffolgenden September beginnt und bis September des darauffolgenden Jahres läuft.

Wenn Sie den Bericht mithilfe der Konsole ausführen, können Sie die folgenden Optionen auswählen:

- Letzte 12 Monate: Die Auswertung umfasst Gebühren von einem Jahr vor der Ausführung des Berichts bis zum aktuellen Tag. Wenn Sie den Bericht beispielsweise am 3. Juni ausführen, umfasst er Gebühren vom 3. Juni des Vorjahres bis zum aktuellen Tag.
- Einzelne Monate im letzten Jahr: Der Bericht enthält Gebühren für den angegebenen Monat.

Wenn Sie den Bericht programmgesteuert ausführen, können Sie Gebühren für jeden Zeitraum ab dem 31. Juli 2014 einschließen. Das ist das Datum, an dem Route 53 mit der Unterstützung der Domainregistrierung begann. Beispiele finden Sie unter Anzeigen in der AWS CLI -Befehlsreferenz.

Der Abrechnungsbericht liegt im CSV-Format vor und der Inhalt wird von der ViewBillingAPI beschrieben.

So laden Sie einen Domains-Rechnungsbericht herunter

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Registered Domains.
3. Wählen Sie Domain billing report.
4. Wählen Sie die Zeitspanne für den Bericht aus, und wählen Sie dann Download domain report.
5. Folgen Sie den Eingabeaufforderungen, um den Bericht zu öffnen oder zu speichern.
6. Wenn beim Herunterladen eines Domain-Abrechnungsberichts Probleme auftreten, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Domains, die Sie mit Amazon Route 53 registrieren können

> **Important**
>
> Die unten aufgeführten Einschränkungen für Top-Level-Domains gelten nur für die Domainregistrierung. Sie können den Route 53-DNS-Dienst mit jeder beliebigen Top-Level-Domain und mit jedem Domain-Registrar verwenden. Die Informationen auf dieser Seite beziehen sich nur auf die Domains, die Sie bei Route 53 registrieren können. Weitere Informationen zur Verwendung von Route 53 als DNS-Service finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird.

Die folgenden Listen generischer und geografischer Top-Level-Domains zeigen die Top-Level-Domains (TLDs), die Sie zur Registrierung von Domains bei Amazon Route 53 verwenden können.

Registrieren von Domains mit Route 53

Bei TLD Registrierungen sind einigen Domainnamen spezielle oder Premium-Preise zugeordnet. Für die Registrierung einer Domain mit einem Spezial- oder Premium-Preis kann Route 53 nicht verwendet werden. Diejenigen TLDs, die Sie bei Route 53 registrieren können, sind in den folgenden Listen enthalten. Wenn die TLD nicht enthalten ist, können Sie die Domain nicht mit Route 53 registrieren.

Übertragen von Domains zu Route 53

Sie können eine Domain in Route 53 übertragen, wenn die TLD in den folgenden Listen enthalten ist. Wenn die TLD nicht enthalten ist, können Sie die Domain nicht in Route 53 übertragen.

In den meisten TLDs Fällen benötigen Sie einen Autorisierungscode vom aktuellen Registrar, um eine Domain zu übertragen. Informationen darüber, ob Sie einen Autorisierungscode benötigen, finden Sie im Abschnitt „Autorisierungscode für Übertragungen erforderlich“ für Ihre TLD.

Preise für Domainregistrierungen und -übertragungen

Informationen zu den Kosten für die Registrierung von Domains oder ihre Übertragung zu Route 53 finden Sie unter Amazon-Route-53-Preise für Domainregistrierung.

Verwendung von Route 53 als Ihr DNS-Service

Sie können Route 53 als DNS-Service für jede Domain verwenden, auch wenn die TLD für die Domain nicht in den folgenden Listen enthalten ist. Weitere Informationen zur Verwendung von Route 53 als DNS-Service finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird. Informationen zum Übertragen des DNS-Service für Ihre Domain an Route 53 finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Internationalisierte Domainnamen

Nicht alle TLDs unterstützen internationalisierte Domainnamen (IDNs), d. h. Domainnamen, die andere Zeichen als die ASCII-Zeichen a-z, 0-9 und - (Bindestrich) enthalten. Die Liste für jede TLD gibt an, ob diese TLD unterstützt. IDNs Weitere Informationen zu internationalisierten Domainnamen finden Sie unter Format für DNS-Domänennamen.

Registrierung geografischer Domains bei TLDs

Die Regeln für die Registrierung geografischer Daten TLDs variieren je nach Land. Einige Länder haben keine Einschränkung. Das bedeutet, dass jeder auf der Welt sich registrieren kann, während andere über bestimmte Einschränkungen verfügen, wie z. B. Residenzanforderungen. Die Auflistung für die einzelnen geografischen TLDs zeigt alle Einschränkungen an.

-Index für unterstützte Top-Level-Domains

Themen

Generische 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, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .beer,.bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .bot, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .weihnachten, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .kontakt, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .kostenlos, .lustig, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .heiß, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .recht, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, .ltd

Mio.

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .moi, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja, .jetzt

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub. .pw (Palau)

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .einkaufen, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .spot, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team, .tech,.technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .abstimmen, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zone

Geografische Top-Level-Domains

Afrika

.ac (Ascension), .co.za (Südafrika), .sh (St. Helena)

Nord- und Südamerika

.ai (Anguilla), .ca (Kanada), .cl (Chile), .co (Kolumbien), .com.ar (Argentinien), .com.br (Brasilien), .com.mx (Mexiko), .mx (Mexiko), .us (USA), .vc (St. Vincent und die Grenadinen), .vg (Britische Jungferninseln)

Asien/Ozeanien

.au (Australien), .cc (Cocos-Inseln (Keeling)), .co.nz (Neuseeland), .com.au (Australien), .com.sg (Republik Singapur), .fm (Föderierte Staaten von Mikronesien), .in (Indien), .jp (Japan), .io

(Britisches Territorium im Indischen Ozean), .net.au (Australien), .net.nz (Neuseeland), .nz (Neuseeland), .org.nz (Neuseeland), .pw (Palau), .qa (Katar), .ru (Russische Föderation), .sg (Republik Singapur)

Europa

.be (Belgien), .berlin (Stadt Berlin, Deutschland), .ch (Schweiz), .co.uk (Großbritannien und Nordirland), .cz (Tschechische Republik), .de (Deutschland), .es (Spanien) , .eu (Europäische Union), .fi (Finnland), .fr (Frankreich), .gg (Guernsey), .im (Isle of Man), .it (Italien), .me (Montenegro), .me.uk (Großbritannien und Nordirland), .nl (Niederlande), .org.uk (Großbritannien und Nordirland), .ruhr (Ruhrgebiet, Westdeutschland), .se (Schweden), .uk (Großbritannien und Nordirland), .wien (Stadt Wien, Österreich)

Generische Top-Level-Domains

Generische Top-Level-Domains (gTLDs) sind globale Erweiterungen, die auf der ganzen Welt verwendet und anerkannt werden, wie z. B. .com, .net und .org. Außerdem umfassen diese spezielle Domains, wie z. B. .bike, .condos und marketing.

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .beer, .bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .bot, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, .weihnachten, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .kontakt, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deal, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .kostenlos, .lustig, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .heiß, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .recht, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , .ltd

Mio.

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .moi, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja, .jetzt

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shop, .einkaufen, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .spot, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team,.tech, .technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .abstimmen, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xxx, .xyz, .zone

.ac

Siehe .ac (Ascension).

Return to index

.academy

Wird von Bildungseinrichtungen wie Schulen und Hochschulen verwenden. Außerdem von Personalvermittler, Beratern, Inserenten, Studenten, Lehrern und Administratoren, die mit Bildungseinrichtungen verbunden sind.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.accountants

Wird von Unternehmen, Gruppen und Personen im Zusammenhang mit Buchhaltung genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.actor

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.adult

Wird für Websites verwendet, deren Inhalte nur für Erwachsene geeignet sind.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.agency

Wird von Unternehmen oder Gruppen genutzt, die sich als Agenturen identifizieren.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.airforce

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.apartments

Wird von Immobilienmaklern, Vermietern und Mietern genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.associates

Wird von Unternehmen und Firmen genutzt, die den Begriff "Associates" in ihrer Bezeichnung tragen. Auch von anderen Gruppen oder Agenturen genutzt, die den professionellen Hintergrund ihrer Organisation verdeutlichen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.auction

Wird für Ereignisse im Zusammenhang mit Auktionen und auktionsbasierten Käufen und Verkäufen genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Spanisch und Latein.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.audio

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .audio-Domains zu registrieren oder .audio-Domains an Route 53 zu übertragen. Die .audio-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird von der audiovisuellen Industrie und Interessenten an Rundfunk, Soundsystemen, Audioproduktion und Audio-Streaming genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .audio-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.band

Wird für die Freigabe von Informationen zu Musikbands und Band-Ereignissen genutzt. Auch von Musikern für den Kontakt zu ihren Fans und zum Verkauf Band-bezogener Waren verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Spanisch und Latein.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bargains

Wird für Informationen über Verkaufs- und Werbeaktionen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.beer

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bet

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bid

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bike

Wird von Unternehmen oder Gruppen genutzt, die Angebote für Zweiradfahrer haben, wie z. B. Fahrradhändler, Motorradhändler und Reparaturwerkstätten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bingo

Wird für Online-Spiele-Websites oder zur Weitergabe von Informationen über das Spiel Bingo verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bio

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.biz

Steht für Unternehmen oder zur gewerblichen Nutzung zur Verfügung.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für vereinfachtes Chinesisch, traditionelles Chinesisch, Dänisch, Finnisch, Deutsch, Ungarisch, Japanisch, Koreanisch, Lettisch, Litauisch, Norwegisch, Polnisch, Portugiesisch, Spanisch und Schwedisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.black

Wird von allen genutzt, die die Farbe Schwarz mögen, oder Unternehmen, die Schwarz mit ihrem Unternehmen oder ihrer Marke verknüpfen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.blue

Wird von allen genutzt, die die Farbe Blau mögen, oder Unternehmen, die Blau mit ihrem Unternehmen oder ihrer Marke verknüpfen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bot

Wird für Chatbot- und KI-bezogene Produkte und Dienstleistungen verwendet. Diese Domainendung hilft dabei, die Natur automatisierter Systeme, Konversationsschnittstellen und neuer Technologien im Bereich der künstlichen Intelligenz zu vermitteln.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.boutique

Wird verwendet, um Informationen über Boutiquen und spezielle kleine Läden bereitzustellen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.builders

Wird von Unternehmen und Personen in der Bauindustrie genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.business

Wird von Firmen und Unternehmen verwendet. Kann alternativ zur Erweiterung .biz verwendet werden.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.buzz

Wird für Informationen über die neuesten Nachrichten und Ereignisse verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cab

Wird von Unternehmen und Personen in der Taxibranche genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cafe

Wird von Cafés und denjenigen, die ein Interesse an Café-Kultur haben, genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.camera

Wird von Fotobegeisterten und allen, die Fotos teilen möchten, genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.camp

Wird für Parks und Naherholungszentren, Ferienlager, Kreativ-Workshops, Fitness-Sommerlager und von Camping-Fans genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.capital

Wird als allgemeine Kategorie für jede Art von Kapital, z. B. Finanzinvestitionen, wie auch für Hauptstädte verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cards

Wird von Unternehmen genutzt, die sich auf Karten spezialisieren, wie z. B. eCards, gedruckte Grußkarten, Visitenkarten und Spielkarten. Auch ideal für Spieler, die über die Regeln und Strategien von Kartenspielen informieren möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.care

Wird von Unternehmen oder Agenturen in der Pflege verwendet. Außerdem von Wohltätigkeits-Organisationen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.careers

Wird für Informationen über die Jobvermittlung verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cash

Wird von Organisationen, Gruppen oder Einzelpersonen mit geldbezogenen Aktivitäten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.casino

Wird von der Glücksspielbranche oder von Spielern, die Informationen zu Glücksspielen und Casino-Spielen teilen möchten, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.catering

Wird von Catering-Unternehmen oder Personen, die Informationen zu kulinarischen Ereignissen teilen möchten, genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cc

Siehe .cc (Cocos-Inseln (Keeling)).

Return to index

.center

Wird als allgemeine Erweiterung für alles von Forschungsunternehmen bis hin zu Stadtteilzentren verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ceo

Wird für Informationen über CEOs und ihresgleichen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Deutsch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.chat

Wird für alle Arten von Online-Chat-Websites genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cheap

Wird von E-Commerce-Websites verwendet, um kostengünstige Produkte zu bewerben und zu verkaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.weihnachten

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Eine späte Verlängerung mit Route 53 ist möglich: Bis 43 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Eine Wiederherstellung mit der Registrierung ist möglich: Zwischen 44 Tagen und 86 Tagen nach Ablauf
- Die Domain wird aus der Registry gelöscht: 86 Tage nach Ablauf

.church

Wird von Kirchen beliebiger Größe und Religion verwendet, um sich mit ihren Gemeinden zu verbinden und um Informationen über kirchliche Ereignisse und Aktivitäten zu veröffentlichen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.city

Wird verwendet, um Informationen zu bestimmten Städten, wie z. B. Sehenswürdigkeiten, Besuchsempfehlungen oder Nachbarschaftsaktivitäten zu veröffentlichen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.claims

Wird von Unternehmen verwendet, die Versicherungsansprüche klären oder juristische Dienstleistungen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cleaning

Wird von Unternehmen oder Personen verwendet, die Reinigungsdienstleistungen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.click

Wird von Unternehmen verwendet, die Klick-Angebote auf ihren Websites haben, z. B. das Klicken auf Produkte auf einer Website, um diese zu kaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Unterstützt.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.clinic

Wird von der Gesundheitsbranche und von medizinischen Fachkräften verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.clothing

Wird von der Modebranche verwendet, einschließlich Händler, Kaufhäuser, Designer, Schneider und Outlets.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cloud

Wird als allgemeine Erweiterung verwendet, ist aber auch ideal für Unternehmen, die Cloud-Computing-Technologien und Services anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.club

Wird von allen Arten von Clubs oder Organisationen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Spanisch und Japanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.coach

Wird von Beratern verwendet, z. B. Sportexperten, Lebensberatern oder Schulungsleitern für Unternehmen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.codes

Wird als allgemeine Erweiterung für alle Arten von Code verwendet, z. B. Verhaltenskodex, Codeaufbau oder Programmiercode.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.coffee

Wird von der Kaffeebranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.college

Wird von Bildungseinrichtungen wie Schulen und Hochschulen verwenden. Außerdem von Personalvermittler, Beratern, Inserenten, Studenten, Lehrern und Administratoren, die mit Bildungseinrichtungen verbunden sind.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, vereinfachtes und traditionelles Chinesisch, Kyrillisch, Griechisch, Hebräisch, Japanisch und Thailändisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.com

Wird für kommerzielle Websites verwendet. Ist die beliebteste Erweiterung im Internet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.community

Wird von beliebigen Communitys, Clubs, Organisationen oder speziellen Interessengruppen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.company

Wird als allgemeine Erweiterung für Unternehmen aller Art verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.computer

Wird als allgemeine Erweiterung für Informationen zu Computern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.condos

Wird von Personen und Unternehmen im Zusammenhang mit Eigentumswohnungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.construction

Wird von der Baubranche, beispielsweise Baufirmen und Auftragnehmern, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.consulting

Wird von Beratern und anderen, die mit der Beratungsbranche zusammenhängen, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, Chinesisch, Französisch, Kyrillisch, Devanagari, Deutsch, Griechisch, Hebräisch, Japanisch, Koreanisch, Latein, Spanisch, Tamilisch und Thai.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kontakt

Wird von Kirchen beliebiger Größe und Religion verwendet, um sich mit ihren Gemeinden zu verbinden und um Informationen über kirchliche Ereignisse und Aktivitäten zu veröffentlichen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.contractors

Wird von Subunternehmern, beispielsweise Auftragnehmern in der Baubranche, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cool

Wird von Organisationen und Gruppen verwendet, die ihre Marke den neuesten Trends zuordnen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.coupons

Wird von Einzelhändlern und Herstellern verwendet, die Online-Gutscheine und Gutscheincodes anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.credit

Wird von der Kreditbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.creditcard

Wird von Unternehmen oder Banken verwendet, die Kreditkarten ausgeben.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.cruises

Wird von der Reisebranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.dance

Wird von Tänzern, Tanzausbildern und Tanzschulen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.dating

Wird für Partnersuche-Websites verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.deal

Wird für Websites verwendet, die Angebote, Rabatte und Sonderangebote anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.deals

Wird verwendet, um Informationen über Online-Schnäppchen und Verkäufe bereitzustellen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.degree

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.delivery

Wird von Unternehmen verwendet, die beliebige Waren oder Dienstleistungen liefern.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.democrat

Wird für Informationen über die Demokratische Partei verwendet. Auch von Vertretern für Wahlbüros, gewählten Volksvertretern, Politikanhängern, Beratern und Spezialisten genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.dental

Wird von Zahnärzten und zahnärztlichen Dienstleistern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.design

Wird von Kirchen beliebiger Größe und Religion verwendet, um sich mit ihren Gemeinden zu verbinden und um Informationen über kirchliche Ereignisse und Aktivitäten zu veröffentlichen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.diamonds

Wird von Diamantenfans und der Diamantenindustrie genutzt, einschließlich Verkäufer, Wiederverkäufer und Händler.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.diet

> **Important**
>
> Sie können Routing nicht mehr verwenden, um neue .diet-Domains zu registrieren oder .diet-Domains an Route 53 zu übertragen. Die .diet-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird von Gesundheits- und Fitness-Experten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .diet-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.digital

Wird für alles digitale verwendet, ist ideal für IT-Unternehmen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.direct

Wird als allgemeine Erweiterung verwendet, eignet sich aber optimal für Nutzer, die Produkte über eine E-Commerce-Website direkt an Kunden verkaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.directory

Wird von der Medienbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.discount

Wird für Rabatt-Websites und Unternehmen, die Preisrabatte anbieten, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.dog

Wird von Hundeliebhabern und Dienstleistungs- und Produktanbietern für Hunde verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.domains

Wird für Informationen über Domainnamen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.education

Wird für Informationen über Bildungsangebote verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.email

Wird für Informationen über Werbe-E-Mails verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.energy

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Nutzer in der Energiewirtschafts- oder Energienachhaltigkeits-Branche.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.engineering

Wird von Technikunternehmen und -experten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.enterprises

Wird für Informationen über Firmen und Unternehmen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.equipment

Wird für Informationen über Anlagen sowie Verleiher, Händler und Hersteller von Zubehör verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.estate

Wird für Informationen über Gebäude und die Wohnungswirtschaft verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.events

Wird für Informationen zu Ereignissen aller Art verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.exchange

Wird für den Austausch aller Daten verwendet: Börsenkurse, Warenhandel oder einfach den Austausch von Informationen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.expert

Wird von Personen mit Spezialkenntnissen in einer Vielzahl von Gebieten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.exposed

Allgemeine Erweiterung für eine Vielzahl von Themen, einschließlich Fotografie, Boulevardpresse und investigativer Journalismus.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.express

Wird als allgemeine Erweiterung verwendet, ist jedoch ideal für Kunden, die auf die schnelle Bereitstellung von Waren oder Dienstleistungen hinweisen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fail

Kann von jedem genutzt werden, der einen Fehler gemacht hat, aber ist ideal für die humorvolle Veröffentlichung von Fehlern und "Fettnäpfchen".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fan

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.farm

Wird von der Landwirtschaft verwendet, beispielsweise Landwirte und Landmaschinentechniker.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.finance

Wird von der Finanzbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.financial

Wird von der Finanzbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fish

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Websites im Zusammenhang mit Fisch und Angeln.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fitness

Wird für Fitness und Fitnessdienstleister verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.flights

Wird von Reisebüros, Fluggesellschaften und Personen aus der Reisebranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.florist

Wird von Floristen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.flowers

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .flowers-Domains zu registrieren oder .flowers-Domains an Route 53 zu übertragen. Die .flowers-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird für alles im Zusammenhang mit Blumen verwendet, z. B. Online-Blumenvertrieb oder Informationen über Blumenanbau und Züchtung.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .flowers-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fm

Siehe .fm (Föderierte Staaten von Mikronesien).

Return to index

.football

Wird von allen verwendet, die etwas mit Fußball zu tun haben.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.forsale

Wird für den Verkauf von Waren und Dienstleistungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.foundation

Wird von gemeinnützigen Organisationen, gemeinnützigen Einrichtungen und Stiftungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kostenlos

Wird für Websites verwendet, die kostenlose Produkte, Dienstleistungen oder Inhalte anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.lustig

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fund

Wird als allgemeine Erweiterung für alles im Zusammenhang mit finanzieller Förderung verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.furniture

Wird von Möbelherstellern und -verkäufern sowie Beteiligten der Möbelindustrie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.futbol

Wird für Informationen über Fußball verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.fyi

Wird als allgemeine Erweiterung verwendet, ist aber ideal für die Verteilung von Informationen aller Art. "FYI" ist eine Abkürzung von "Für Ihre Informationen".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gallery

Wird von Inhabern von Kunstgalerien verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.games

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gift

Wird von Unternehmen oder Organisationen verwendet, die Geschenke oder geschenkbezogene Dienstleistungen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gifts

Wird von Unternehmen oder Organisationen verwendet, die Geschenke oder geschenkbezogene Dienstleistungen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gives

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.glass

Wird von der Glasindustrie wie Glasschleifern und Fensterinstallateuren verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.global

Wird von Unternehmen oder Gruppen mit einem internationalen Markt oder internationaler Vision verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, Weißrussisch, Bosnisch, Bulgarisch, Chinesisch (vereinfacht), Chinesisch (traditionell), Dänisch, Deutsch, Indisch, Ungarisch, Isländisch, Koreanisch, Lettisch, Litauisch, Mazedonisch, Montenegrinisch, Polnisch, Russisch, Serbisch, Spanisch, Schwedisch und Ukrainisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gmbh

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gold

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Unternehmen, die Produkte im Zusammenhang mit Gold kaufen oder verkaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.golf

Wird für Websites im Zusammenhang mit Golf verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.graphics

Wird von der Grafikbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gratis

Wird für Websites verwendet, die kostenlose Produkte anbieten, wie Werbeartikel, Downloads oder Coupons. "Gratis" bedeutet "kostenlos".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.green

Wird für Websites im Zusammenhang mit Umweltschutz, Ökologie, die Umwelt und einem "grünen" Lebensstil verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.gripe

Wird für die Weitergabe von Beschwerden und Kritik verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.group

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.guide

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Websites, die sich auf Reiseziele, Reisedienstleistungen und -produkte beziehen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.guitars

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .guitars-Domains zu registrieren oder .guitars-Domains an Route 53 zu übertragen. Die .guitars-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird von Gitarrenfans verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .guitars-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.guru

Wird von Nutzern verwendet, die ihr Wissen zu einer Reihe von Themen weitergeben möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.haus

Wird von der Immobilien- und Baubranche verwendet. "haus" steht ganz einfach für "Haus".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.healthcare

Vom Gesundheitswesen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.help

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Websites, die Online-Hilfe und Informationen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.hiv

Wird für Websites verwendet, die sich dem Kampf gegen HIV widmen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.hockey

Wird für Websites im Zusammenhang mit Hockey verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.holdings

Wird von Finanzberatern, Börsianern und Investoren verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.holiday

Wird von der Reisebranche und Personen und Unternehmen im Zusammenhang mit der Planung von Partys und besonderen Anlässen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.host

Wird von Unternehmen verwendet, die Web-Hosting-Plattformen und -Services anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Griechisch, Hebräisch, Koreanisch und Thai.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.hosting

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .hosting-Domains zu registrieren oder .hosting-Domains zu Route 53 zu übertragen. Die .hosting-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird für das Hosten von Websites und in der Hosting-Branche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .hosting-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.heiß

Wird für Websites mit Trendthemen, beliebten Inhalten oder zeitkritischen Angeboten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.house

Wird von Immobilienmaklern sowie Käufern und Verkäufern von Häusern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.im

Siehe .im (Isle of Man).

Return to index

.immo

Wird von der Immobilienbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.immobilien

Wird für Informationen über Immobilien verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.industries

Wird von Unternehmen oder kommerziellen Großunternehmen verwendet, die sich als Industrie identifizieren.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.info

Wird für die Verbreitung von Informationen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ink

Wird von Tattoo-Fans oder Branchen im Zusammenhang mit Tinte, z. B. der Druck- und Verlagsbranche, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch und Latein.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.institute

Wird von beliebigen Organisationen oder Gruppen verwendet, vor allem von Forschungs- und Bildungseinrichtungen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.insure

Wird von Versicherungsgesellschaften und Versicherungsvermittlern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.international

Wird von Unternehmen verwendet, die internationale Zweigstellen haben, Auslandsreisenden oder Wohltätigkeitsorganisationen mit internationalem Einfluss.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.investments

Wird als allgemeine Erweiterung verwendet, ist aber ideal für die Bekanntmachung von Investitionsmöglichkeiten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.io

Siehe .io (Britisches Territorium im Indischen Ozean).

Return to index

.irish

Dient zur Förderung der irischen Kultur und irischen Organisationen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Französisch, Deutsch, Griechisch, Hebräisch, Japanisch, Koreanisch, Spanisch, Tamilisch und Thai.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.jewelry

Wird von Schmuckverkäufern und -käufern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.juegos

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .juegos-Domains zu registrieren oder .juegos-Domains an Route 53 zu übertragen. Die .juegos-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Wird für Gaming-Websites aller Arten verwendet. "Juegos" ist Spanisch für "Spiele".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .juegos-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kaufen

Wird für Informationen über E-Commerce verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kim

Wird von Personen verwendet, deren Vor- oder Nachname Kim ist.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kitchen

Wird von Küchenhändlern, Köchen, Food-Bloggern und Personen in der Lebensmittelindustrie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.kiwi

Wird von Unternehmen und Personen verwendet, die Neuseelands Kiwi-Kultur unterstützen möchten. Dient außerdem als Plattform für die humanitäre Unterstützung des Wiederaufbaus von Christchurch, das durch Erdbeben 2010 und 2011 beschädigt wurde.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Maori.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.land

Wird von Landwirten, Immobilienmaklern, kommerziellen Entwicklern und Interessenten an Immobilienanlagen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.recht

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.lease

Wird von Immobilienmaklern, Vermietern und Mietern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.legal

Wird von Mitgliedern der Rechtsberufe verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.lgbt

Wird von der Gemeinschaft lesbischer, schwuler, bisexueller und transsexueller Menschen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.life

Wird als allgemeine Erweiterung verwendet und eignet sich für eine Vielzahl von Unternehmen, Gruppen und Personen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.lighting

Wird von Fotografen, Designern, Architekten, Technikern und andere Personen mit Interesse an Beleuchtung verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.limited

Wird als allgemeine Erweiterung verwendet und eignet sich für eine Vielzahl von Unternehmen, Gruppen und Personen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.limo

Wird von Chauffeuren, Limousinenvermietern und Autovermietungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.link

Wird für Informationen über die Erstellung von Online-Verknüpfungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Uniregistry ist die Registrierung für .LINK-Domains. Aufgrund der Uniregistrierungs-Richtlinie zeigt die Registry-Ebene WHOIS „REDACTED FOR PRIVACY“ (Für den Datenschutz unkenntlich gemacht) an. Das Entfernen unseres Datenschutzfeatures wirkt sich nur auf die Informationen aus, die auf der Registrarebene Amazon-Registrar WHOIS angezeigt werden.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.live

Wird als allgemeine Erweiterung verwendet und eignet sich für eine Vielzahl von Unternehmen, Gruppen und Personen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.llc

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.loan

Wird von Kreditgebern, Kreditnehmern sowie dem Kreditgewerbe verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Dänisch, Deutsch, Norwegisch und Schwedisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.loans

Wird von Kreditgebern, Kreditnehmern sowie dem Kreditgewerbe verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.lol

Wird für Humor- und Comedy-Websites verwendet. "LOL" ist eine Abkürzung für "laut lachen".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch, Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ltd

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.maison

Wird von der Immobilienbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.management

Wird für Informationen über die Geschäftswelt und das Unternehmens-Management verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.marketing

Wird vom Marketing-Sektor für eine Vielzahl von Zwecken verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.mba

Wird für Websites verwendet, die Informationen über den Master in Business Administration (MBA) bereitstellen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.media

Wird von der Medien- und Unterhaltungsbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.memorial

Wird von Gedenkorganisationen zum Gedenken an Ereignisse und Personen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.mobi

Wird von Unternehmen und Personen verwendet, die ihre Websites für Smartphones optimieren möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.moda

Wird für Informationen über Mode verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.moi

Französisch für „ich“. Wird verwendet, um französischsprachigen Endnutzern französischsprachige Inhalte zu signalisieren. Geeignet für persönliche Blogs CVs, Portfolios und Hobby- oder Interessensseiten auf Französisch.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Unterstützt.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.money

Wird für Websites verwendet, die sich auf Geld und geldbezogene Aktivitäten konzentrieren.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.mortgage

Wird von der Hypothekenbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.movie

Wird für Websites verwendet, die Informationen über Filme und Filmproduktionen bereitstellen. Geeignet für Profis und Fans.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.name

Wird von allen verwendet, die eine personalisierte Webpräsenz erstellen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Mit Verisign, der Registry für.name TLDs, können Sie sowohl Domains zweiter Ebene (Name .name) als auch Domains dritter Ebene (Vorname) registrieren. Nachname (.name). Route 53 unterstützt nur Domains zweiter Ebene, sowohl für die Registrierung von Domains als auch für die Übertragung von vorhandenen Domains in Route 53.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.net

Wird für alle Arten von Websites verwendet. Die .net-Erweiterung ist eine Abkürzung für Netzwerk.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.network

Wird in der Netzwerkbranche oder zum Einrichten von Verbindungen über Netzwerke verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.news

Wird für die Verteilung von beachtenswerten Informationen wie aktuelle Veranstaltungen oder Informationen, die sich auf Journalismus und Kommunikation beziehen, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ninja

Wird von Personen und Unternehmen verwendet, die sich mit den Fähigkeiten eines Ninjas identifizieren möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.jetzt

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.onl

Die .onl-Erweiterung ist eine Abkürzung für "Online", und steht außerdem in Spanisch für gemeinnützige Organisationen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.online

Die .onl-Erweiterung ist eine Abkürzung für "Online", und steht außerdem in Spanisch für gemeinnützige Organisationen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.org

Wird von allen möglichen Organisationen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.partners

Wird von Anwaltskanzleien, Investoren und einer Vielzahl von Unternehmen verwendet. Gilt auch für Websites, die Beziehungen aufbauen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.parts

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Teilehersteller, Verkäufer und Käufer.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.photo

Wird von Fotografen und Fotointeressenten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.photography

Wird von Fotografen und Fotointeressenten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.photos

Wird von Fotografen und Fotointeressenten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pics

Wird von Fotografen und Fotointeressenten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pictures

Wird von Fotografen und Interessenten an Fotografie, Kunst und Medien verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pink

Wird von allen genutzt, die die Farbe Pink mögen, oder Unternehmen, die Pink mit ihrem Unternehmen oder ihrer Marke verknüpfen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pizza

Wird von Pizzarestaurants und Pizzafans verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.place

Wird als allgemeine Erweiterung verwendet, ist aber ideal für die Wohneigentums- und Reisebranche.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.plumbing

Wird von der Sanitärbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.plus

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Bekleidung in Plus-Größen, zusätzliche Software oder Produkte, die "Extra"-Funktionen oder Dimensionen anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.poker

Wird von Pokerspielern und Gaming-Websites verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.porn

Wird für Erwachsenen-Websites verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.press

Wird für Erwachsenen-Websites verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pro

Wird von lizenzierten und zugelassenen Experten und professionellen Organisationen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.productions

Wird von Studios und Produktionshäusern verwendet, die Werbespots, Radiowerbung und Musikvideos produzieren.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.properties

Wird verwendet, um Informationen zu Eigentum, einschließlich Immobilien oder geistiges Eigentum, bereitzustellen. Auch von Personen verwendet, die Häuser, Gebäude oder Grundstücke verkaufen, vermieten oder mieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.property

Wird verwendet, um Informationen zu Eigentum, einschließlich Immobilien oder geistiges Eigentum, bereitzustellen. Auch von Personen verwendet, die Häuser, Gebäude oder Grundstücke verkaufen, vermieten oder mieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .property-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.pub

Wird von Verlagen, Werbeagenturen oder Kneipen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.qpon

Wird für Coupons und Gutscheincodes verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.recipes

Wird von Personen verwendet, die Rezepte weitergeben möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.red

Wird von allen genutzt, die die Farbe Rot mögen, oder Unternehmen, die Rot mit ihrem Unternehmen oder ihrer Marke verknüpfen wollen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.reise

Wird für Websites im Zusammenhang mit Reisen oder Ausflügen verwendet. "Reise" kann auch als "sich auf den Weg begeben" gedeutet werden.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.reisen

Wird für Websites im Zusammenhang mit Reisen oder Ausflügen verwendet. „Reisen“ ist ein deutsches Wort, das „to travel“ (reisen) bedeutet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.rentals

Wird für alle Arten von Vermietungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.repair

Wird von Reparaturservices oder Personen, die ihr Wissen über alle möglichen Reparaturen weitergeben möchten, verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.report

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Informationen über Unternehmensberichte, Community-Publikationen, Buchrezensionen oder Nachrichten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.republican

Wird für Informationen über die Republikanische Partei verwendet. Auch von Vertretern für Wahlbüros, gewählten Volksvertretern, Politikanhängern, Beratern und Spezialisten genutzt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.restaurant

Wird von der Restaurantbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.reviews

Wird von Personen verwendet, die ihre Meinung kundtun und die Kommentare anderer lesen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.rip

Wird für Websites im Zusammenhang mit dem Tod und mit Grabsteinen verwendet. "RIP" ist eine Abkürzung für "Ruhe in Frieden".

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.rocks

Wird als allgemeine Erweiterung verwendet, ist aber ideal für alle, die "rocken" oder sich mit Steinen beschäftigen: Musiker, Geologen, Juweliere, Kletterer und viele mehr.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.run

Wird als allgemeine Erweiterung verwendet, ist aber ideal für die Sport- und Fitnessbranche.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.sale

Wird von E-Commerce-Websites verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.sarl

Wird von Aktiengesellschaften in der Regel in Frankreich verwendet. "SARL" ist eine Abkürzung für Société à Responsabilité Limité.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.school

Wird für Informationen über Ausbildung, Bildungseinrichtungen und schulische Aktivitäten verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.schule

Wird für Informationen über Ausbildung, Bildungseinrichtungen und schulische Aktivitäten in Deutschland verwendet. "Schule" bezieht sich auf deutsche Schulen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.services

Wird für Websites verwendet, die alle Arten von Services anbieten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.sex

Wird für Websites verwendet, deren Inhalte nur für Erwachsene geeignet sind.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.sexy

Wird für sexuelle Inhalte verwendet. Dient jedoch auch für die Beschreibung der beliebtesten und spannendsten Marken, Produkte, Informationen und Websites.

Return to index

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .sexy-Domains zu registrieren oder .sexy-Domains an Route 53 zu übertragen. Die .sexy-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .sexy-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.shiksha

Wird von Bildungseinrichtungen verwendet. "Shiksha" ist eine indische Bezeichnung für Schulen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.shoes

Wird von Schuhläden, Designern, Hersteller oder Mode-Bloggern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.shop

Wird für Online- und brick-and-mortar Einzelhandelsunternehmen sowie für Dienstleister verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.einkaufen

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.show

Wird als allgemeine Erweiterung verwendet, ist aber ideal für die Unterhaltungsbranche.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.singles

Wird von Partnersuchdiensten, Ferienanlagen und anderen Unternehmen verwendet, die andere bei der Partnersuche unterstützen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.site

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ski

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.soccer

Wird für Websites im Zusammenhang mit Fußball verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.social

Wird für Informationen über soziale Medien, Foren und Online-Chats verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.solar

Wird für Informationen über das Sonnensystem und Sonnenenergie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.solutions

Wird von Beratern, do-it-yourself Dienstleistungen und Beratern aller Art verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.software

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.space

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.spot

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.store

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.stream

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.studio

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Nutzer in der Immobilien-, Kunst- oder Unterhaltungsbranche.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.style

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Websites mit Schwerpunkt auf den neuesten Trends, vor allem Trends in Mode, Design, Architektur und Kunst.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.sucks

Wird als allgemeine Erweiterung verwendet, eignet sich aber optimal für Nutzer, die negative Erfahrungen weitergeben möchten oder andere vor Betrug, Etikettenschwindel oder fehlerhaften Produkten warnen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.supplies

Wird von Unternehmen verwendet, die Produkte online verkaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.supply

Wird von Unternehmen verwendet, die Produkte online verkaufen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.support

Wird von Unternehmen, Gruppen oder Wohltätigkeitsorganisationen verwendet, die Unterstützung anbieten, einschließlich Kunden-, Produkt- oder Systemsupport sowie emotionale, finanzielle oder geistige Unterstützung.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.surgery

Wird für Informationen zu Operationen, Medizin und Gesundheit verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.systems

Wird vorrangig von der IT-Branche und Anbietern von IT-Services verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tattoo

Wird von Tattoo-Fans und der Tätowierungsbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Kyrillisch (in erster Linie Russisch), Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tax

Wird für Informationen zu Steuern, Steuerberatung und Steuerrecht verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.taxi

Wird von Taxis, Chauffeuren und Shuttle-Unternehmen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.team

Wird von Unternehmen oder Organisationen verwendet, die sich als Team identifizieren.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tech

Wird von Technologiebegeisterten und Unternehmen, Services und Herstellern mit Schwerpunkt auf Technologie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.technology

Wird von Technologiebegeisterten und Unternehmen, Services und Herstellern mit Schwerpunkt auf Technologie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tennis

Wird für Informationen zu Tennis verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.theater

Wird für Websites mit Schwerpunkt auf Theater, Schauspiel und Musicals verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tienda

Wird von Unternehmen im Einzelhandel verwendet, um eine Verbindung mit spanischsprachigen Kunden herzustellen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tips

Wird von Nutzern verwendet, die an ihre Kenntnisse und Ratschläge zu praktisch jedem Thema weitergeben möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tires

Wird von Herstellern, Lieferanten oder Käufer von Reifen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.today

Wird für Informationen über aktuelle Veranstaltungen, Nachrichten, Wetter, Unterhaltung und vieles mehr verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tools

Wird für Informationen zu allen Arten von Werkzeugen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tours

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Reiseunternehmen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.town

Wird verwendet, um das Lokalkolorit, die Kultur und die Kommune einer Stadt vorzustellen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.toys

Wird von der Spielzeugindustrie verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.trade

Wird als allgemeine Erweiterung verwendet, ist aber ideal für kommerzielle Websites oder Handelsdienstleister.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Dänisch, Deutsch, Norwegisch und Schwedisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.training

Wird von Trainern, Ausbildern und Pädagogen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.tv

Wird für Informationen über Fernsehen und Medien verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Keine.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.university

Wird von Universitäten und anderen Bildungseinrichtungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.uno

Wird für Informationen über spanische, portugiesische und italienische Communitys verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.vacations

Wird von der Reise- und Tourismusbranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.vegas

Dient zur Werbung für die Stadt Las Vegas und den Las Vegas-Lifestyle.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ventures

Wird von Jungunternehmern, Startups, Risikokapitalgebern, Investmentbanken und Finanziers verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.vg

Siehe .vg (Britische Jungferninseln).

Return to index

.viajes

Wird von Reisebüros, Reiseunternehmen, Reise-Blogs, Touristikunternehmen, Mietservices, Reise-Bloggern und Reiseanbietern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.video

Wird von der Medien- und Videobranche verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Chinesisch, Französisch, Deutsch, Latein und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.villas

Wird von Immobilienmaklern und Grundstückseigentümern verwendet, die Villen verkaufen, vermieten oder leasen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.vision

Wird als allgemeine Erweiterung verwendet, ist aber ideal für Augenspezialisten wie Augenoptiker und Augenärzte.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.abstimmen

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.voyage

Wird von Reisebüros, Reiseunternehmen, Reise-Blogs, Touristikunternehmen, Mietservices, Reise-Bloggern und Reiseanbietern verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.watch

Wird für Informationen über Streaming-Websites, Websites TVs, Videos oder Uhren verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.website

Wird für Informationen über Website-Entwicklung, Werbung, Verbesserungen und Erfahrungen verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Griechisch, Hebräisch, Japanisch, Koreanisch und Thai.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf

- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.wedding

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Keine.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Für Chinesisch, Französisch, Deutsch und Spanisch unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.wiki

Wird für Informationen über Online-Dokumentation verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch und Latein.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.wine

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz

Unterstützt.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.work

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.works

Wird von Unternehmen, Organisationen und Einzelpersonen für Informationen zum Arbeitsleben, zu Jobs und Jobservices verwendet. Diese Erweiterung kann als Alternative zu den Erweiterungen .com, .net oder .org verwendet werden.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.world

Wird von Nutzern verwendet, die Informationen zu globalen Themen bereitstellen möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.wtf

Kann von jedem verwendet werden, der sich mit der beliebten (aber unanständigen) Abkürzung "WTF" (What the fuck) identifizieren möchte.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.xxx

Wird für Websites verwendet, deren Inhalte nur für Erwachsene geeignet sind.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.xyz

Wird als allgemeine Erweiterung für einen beliebigen Zweck verwendet.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Die Registry für .xyz-Domains, Generation XYZ, betrachtet einige Domainnamen als Premium-Domainnamen. Sie können keine .xyz-Premium-Domains in Route 53 registrieren oder übertragen. Weitere Informationen finden Sie auf der Website von Generation XYZ.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.zone

Wird für Informationen über jede Art von Zone verwendet, einschließlich Zeitzonen, Klimazonen und Ostzonen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Französisch und Spanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

Geografische Top-Level-Domains

Die folgenden Domainendungen sind nach Regionen gruppiert und beinhalten offizielle länderspezifische Erweiterungen, sogenannte länderspezifische Top-Level-Domains (ccTLDs). Zu den Beispielen gehören .be (Belgien), .in (Indien) und .mx (Mexiko). Die Regeln für die Registrierung von cc TLDs variieren je nach Land. Einige Länder haben keine Einschränkung. Das bedeutet, dass jeder auf der Welt sich registrieren kann, während andere über bestimmte Einschränkungen verfügen, wie z. B. Residenzanforderungen. Die Auflistung für die einzelnen ccTLDs zeigt alle Einschränkungen an.

> **Important**
>
> Bei der Übertragung von CC TLDs auf Route 53, mit Ausnahme von .cc und .tv, werden Aktualisierungen des Eigentümerkontakts ignoriert und die Kontaktdaten des Besitzers aus der Registrierung verwendet. Sie können die Kontaktinformationen des Eigentümers aktualisieren, nachdem die Übertragung abgeschlossen ist. Weitere Informationen finden Sie unter Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne.

Return to index

Afrika

.ac (Ascension), .co.za (Südafrika), .sh (St. Helena)

Nord- und Südamerika

.ai (Anguilla), .ca (Kanada), .cl (Chile), .co (Kolumbien), .com.ar (Argentinien), .com.br (Brasilien), .com.mx (Mexiko), .mx (Mexiko), .us (USA), .vc (St. Vincent und die Grenadinen), .vg (Britische Jungferninseln)

Asien/Ozeanien

.au (Australien), .cc (Cocos-Inseln (Keeling)), .co.nz (Neuseeland), .com.au (Australien), .com.sg (Republik Singapur), .fm (Föderierte Staaten von Mikronesien), .in (Indien), .jp (Japan), .io (Britisches Territorium im Indischen Ozean), .net.au (Australien), .net.nz (Neuseeland), .nz (Neuseeland), .org.nz (Neuseeland), .pw (Palau), .qa (Katar), .ru (Russische Föderation), .sg (Republik Singapur)

Europa

.be (Belgien), .berlin (Stadt Berlin, Deutschland), .ch (Schweiz), .co.uk (Großbritannien und Nordirland), .cz (Tschechische Republik), .de (Deutschland), .es (Spanien) , .eu (Europäische Union), .fi (Finnland), .fr (Frankreich), .gg (Guernsey), .im (Isle of Man), .it (Italien), .me (Montenegro), .me.uk (Großbritannien und Nordirland), .nl (Niederlande), .org.uk (Großbritannien und Nordirland), .ruhr (Ruhrgebiet, Westdeutschland), .se (Schweden), .uk (Großbritannien und Nordirland), .wien (Stadt Wien, Österreich)

Afrika

Sie können die folgenden Top-Level-Domains (TLDs) für Afrika verwenden, um Domains bei Amazon Route 53 zu registrieren.

, ,

Return to index

.ac (Ascension)

Return to index

Auch als generische TLD verwendet, beliebt bei Nutzern aus der akademischen Welt.

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 80 Tage nach Ablauf

.co.za (Südafrika)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Nur Domains zweiter Ebene stehen für die .za-Erweiterung zur Verfügung. Route 53 unterstützt die Domain zweiter Ebene .co.za.

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die Registrierung steht identifizierbaren Rechtspersonen (Personen und juristischen Personen) offen.
- Der Domainname muss während des Registrierungsvorgangs eine Zonenüberprüfung bestehen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Nein

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu einem Tag vor dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: 1 Tag vor Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 1 Tag und 9 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 9 Tage nach Ablauf

.sh (St. Helena)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 80 Tage nach Ablauf

Nord- und Südamerika

Sie können die folgenden Top-Level-Domains (TLDs) für Amerika verwenden, um Domains bei Amazon Route 53 zu registrieren.

, , , , , , , , , ,

Return to index

.ai (Anguilla)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Registrierung: Zwei bis zehn Jahre. Verlängerung: Zwei bis neun Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Eine späte Verlängerung mit Route 53 ist möglich: Bis 45 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.ca (Kanada)

Return to index

Varianten eines Domainnamens mit (à) oder ohne (a) eines Akzents sind automatisch für den Registranten reserviert und werden Teil eines Verwaltungspakets. Um eine Domain in einem Paket

zu aktivieren, muss der Registrant eine Registrierungsanfrage für die Domain stellen. Alle Domains innerhalb eines Pakets müssen von demselben Registranten und demselben Registrar registriert werden. Der Registrant muss außerdem eine Übertragungsanfrage für alle Domains in einem Paket einreichen, um die Übertragung abzuschließen.

Bestätigungs-E-Mail von der TLD-Registrierungsstelle

Wenn Sie eine .ca-Domain registrieren, erhalten Sie eine E-Mail mit einem Link zum Genehmigungsverfahren der Registrierendenvereinbarung. Sie müssen den Vorgang innerhalb von sieben Tagen abschließen, andernfalls wird Ihre Domain nicht registriert.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die Registrierung ist offen für Personen oder Organisationen in Verbindung mit Kanada, gemäß den kanadischen Präsenzanforderungen für Registrierende.
- Registrierendenkontakt: Sie müssen den vollständigen, genauen rechtlichen Namen des Eigentümers der Domain angeben.
- Admin und technischer Kontakt: Sie müssen eine Person als Kontakttyp angeben und Kontaktinformationen von Personen, die in Kanada leben, eintragen.
- Wählen Sie eine der folgenden Rechtsformen während des Registrierungsvorgangs aus:
  - ABO: Ureinwohner (Einzelpersonen oder Gruppen) in Kanada
  - ASS: Kanadischer Verein ohne Rechtspersönlichkeit
  - CCO: Kanadische Körperschaft oder kanadische Provinz oder Territorium
  - CCT: Kanadischer Staatsbürger
  - EDU: Kanadische Bildungseinrichtung
  - GOV: Regierung oder Regierungsbehörde in Kanada
  - HOP: Kanadisches Krankenhaus
  - INB: Durch den Indian Act of Canada anerkannte Indian Band
  - LAM: Kanadische(s) Bibliothek, Archiv oder Museum
  - LGR: Rechtsvertreter eines kanadischen Staatsbürgers oder einer Person mit ständigem Wohnsitz in Kanada
  - MAJ: Her/His Majestät die Königin/der König

- OMK: Offizielle in Kanada eingetragene Marke
- PLT: Kanadische politische Partei
- PRT: In Kanada registrierte Partnerschaft
- RES: Person mit ständigem Wohnsitz in Kanada
- TDM: Handelsmarke, die in Kanada registriert ist (von nicht kanadischen Eigentümertyp)
- TRD: Kanadische Gewerkschaft
- TRS: In Kanada gegründeter Trust

Datenschutz

- Person — Bei allen Kontakten werden Kontaktname, Adresse, Telefonnummer, Faxnummer und E-Mail-Adresse ausgeblendet, da CIRA den Datenschutz automatisch auf eine Person anwendet. Die Datenschutzoption wird nur beim Whois des Registrars angewendet.
- Unternehmen, Vereinigung oder öffentliche Einrichtung — Wird auf Registrierungsebene nicht unterstützt.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: variiert. AWS Support kontaktieren.

Löschen der Domainregistrierung

Die Registrierungsstelle für .ca-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.cl (Chile)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .cl-Domains zu registrieren oder .cl-Domains an Route 53 zu übertragen. Die .cl-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Zwei Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .cl-Domains mehr in Route 53 übertragen.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Erneuerung möglich: Wenden Sie sich an den AWS -Support.

- Späte Verlängerung mit Route 53 möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus Route 53: gelöscht: Wenden Sie sich an AWS -Support.
- Wiederherstellung mit der Registrierung möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

.co (Kolumbien)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz (gilt für: Person)

Alle Informationen sind verborgen.

Wenn es sich bei dem Kontakttyp nicht um eine Person handelt, werden Firmenname und Land von WHOIS angezeigt.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 45 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 50 Tage nach Ablauf

.com.ar (Argentinien)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .com.ar-Domains zu registrieren oder .com.ar-Domains an Route 53 zu übertragen. Die .com.ar-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Ein Jahr.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Um unbefugte Übertragungen zu verhindern, schränken Sie den Zugriff auf die E-Mail-Adresse des Registranten und die Route 53 ein APIs , da dies beispielsweise zu einem Eigentümerwechsel führen könnte. UpdateDomainContact Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domains in der Service-Autorisierungs-Referenz und Beispielberechtigungen für einen Domänendatensatzbesitzer.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .com.ar-Domains mehr in Route 53 übertragen.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Erneuerung möglich: Wenden Sie sich an den AWS -Support.

- Späte Verlängerung mit Route 53 möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus Route 53: gelöscht: Wenden Sie sich an AWS -Support.
- Wiederherstellung mit der Registrierung möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

.com.br (Brasilien)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .com.br-Domains zu registrieren oder .com.br-Domains an Route 53 zu übertragen. Die .com.br-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Ein Jahr.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .com.br-Domains mehr in Route 53 übertragen.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 30 Tagen vor Ablauf und dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 119 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 119 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 119 Tage nach Ablauf

.com.mx (Mexiko)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.mx (Mexiko)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.us (USA)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Die Registrierung für .us-Domains erlaubt keine Domainnamen mit einem der sieben Wörter aus dem „Appendix to Opinion of the Court“ des Federal Communications Commission v. Pacifica Foundation No 77-528.

Für die Öffentlichkeit nutzbar, mit einer Einschränkung:

- Die .us-Erweiterung gilt für Websites oder Aktivitäten, die sich in den Vereinigten Staaten von Amerika befinden.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 65 Tage nach Ablauf

.vc (St. Vincent und die Grenadinen)

Wird auch als generische TLD verwendet, oft von Beteiligten an Risikokapitalfinanzierungen, Universitäten und so weiter.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 80 Tage nach Ablauf

.vg (Britische Jungferninseln)

Wird auch als generische TLD verwendet, häufig von Unternehmen im Zusammenhang mit Videospielen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu 44 Tage nach dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Ja
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Domain wird aus der Registrierung gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 74 Tagen nach Ablauf
- Domain wird wieder öffentlich zugänglich gemacht: 80 Tage nach Ablauf

Asien/Ozeanien

Sie können die folgenden Top-Level-Domains (TLDs) für Asien und Ozeanien verwenden, um Domains bei Amazon Route 53 zu registrieren.

, , , , , , , , , , , , , , ,

Return to index

.au (Australien)

Return to index

Bestätigungs-E-Mail von der TLD-Registrierungsstelle

Unser Registrar-Mitarbeiter, Gandi, verkauft AU-Domains weiter über. DomainDirectors Wenn Sie einen Domainnamen auf Route 53 übertragen, DomainDirectors sendet er eine E-Mail an den Ansprechpartner des Registranten für die Domain, um die Kontaktinformationen zu überprüfen oder Übertragungsanfragen zu autorisieren.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die .au-Domains sind offen für juristische Personen, Handelsunternehmen, Partnerschaften oder Einzelfirmen, die in Australien registriert sind, ausländische Unternehmen mit Handelslizenz in Australien; sowie Eigentümer oder Anmelder einer in Australien registrierten Handelsmarke. Einzelpersonen können keine .au-Domains registrieren. Der Kontakt des Registranten muss ein Unternehmen sein.
- Während des Registrierungsvorgangs müssen Sie Folgendes angeben:
  - Ihr Registrierungstyp: ABN (australische Geschäftsnummer), ACN (australische Firmennummer) oder TM (Marke), wenn der Domainname Ihrer Marke entspricht.
  - Ihre ID-Nummer, bei der es sich um einen australischen Unternehmensnamen (ABN), eine australische Unternehmensnummer (ACN) oder eine TM (Marke) handeln kann.
  - Ihr Registrantenname, der der Name der juristischen Person ist, die die Domains registriert. Dieser Wert muss exakt mit dem Namen auf der angegebenen ABN (Australian Business Number), ACN (Australian Company Number) oder TM (Trademark) übereinstimmen.

- Ihr Berechtigungstyp, der sich auf die Art der juristischen Person bezieht, die den Domainnamen registriert.
- Der Grund, warum Sie diesen Domainnamen registrieren dürfen (politischer Grund):
  - Der Domainname entspricht dem Akronym oder der Abkürzung des Unternehmens- oder Handelsnamens, des Organisations- oder Verbandsnamens oder der Marke des Registranten. (Politischer Grund 1)
  - Der Domainname entspricht den Zuteilungsregeln, ist jedoch kein Akronym oder eine Abkürzung für den Firmen- oder Handelsnamen, den Organisations- oder Verbandsnamen oder die Marke des Registranten. (Politischer Grund 2). Die Zuweisungsregeln für .au finden Sie in SCHEDULE A in der .au-Registrierung.
- Falsche oder nicht übereinstimmende Kontaktinformationen, einschließlich Name, ABN oder Markennummer (TM), führen zu Fehlern bei der Registrierung, beim Handel und bei Verlängerungen. Möglicherweise ist eine Eigentümeränderung erforderlich, um Informationen für vorhandene Domains zu korrigieren.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja. Neben der Route 53-Konsole können Sie den Übertragungscode auch in der .au-Registrierung abrufen.

DNSSEC

Für die Domainregistrierung unterstützt. Wenn Sie den Schlüssel festlegen, müssen Sie den DNS-Sicherheitsalgorithmus 2 (DH) wählen. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 60 Tagen vor Ablauf und dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 29 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 30 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .au-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

Ändern der Eigentümerschaft

Ändern Sie den Besitzer über die Route-53-Konsole. Siehe Aktualisieren der Kontaktinformationen für eine Domäne. Führen Sie dann den folgenden Vorgang ab, um die Besitzeränderung abzuschließen:

1. Sowohl der alte als auch der neue Registrant müssen auf den Link klicken, den sie in einer E-Mail von transfers@1api.net an ihre angegebenen E-Mail-Adressen erhalten. Wenn dies nicht innerhalb von 14 Tagen abgeschlossen ist, müssen Sie den Vorgang erneut starten.

2. Nachdem die Antworten bestätigt wurden, wird die Besitzeränderung in der Registrierung in kurzer Zeit ohne weitere Bestätigung bearbeitet.

.cc (Cocos-Inseln (Keeling))

Return to index

Wird auch als generische TLD verwendet, häufig von Unternehmen mit "cc" in ihrem Namen, z. B. Consulting-Unternehmen, Cloud-Computing-Anbieter oder Champagner-Hersteller. Die Erweiterung ist eine beliebte Alternative zu ".com".

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

- Ausgeblendet – Adresse, Telefonnummer, Faxnummer und E-Mail-Adresse
- Nicht ausgeblendet – Kontaktname und Organisationsname

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 65 Tage nach Ablauf

.co.nz (Neuseeland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen mindestens 18 Jahre alt sein.

- Organisationen müssen registriert sein.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: zwischen 44 und 134 Tagen nach Ablauf
- Löschung der Domain aus der Registrierung: 134 Tage nach Ablauf

.com.au (Australien)

Return to index

Bestätigungs-E-Mail von der TLD-Registrierungsstelle

Unser Registrar-Mitarbeiter, Gandi, verkauft .com.au-Domains weiter über. DomainDirectors Wenn Sie einen Domainnamen auf Route 53 übertragen, DomainDirectors sendet er eine E-

Mail an den Ansprechpartner des Registranten für die Domain, um die Kontaktinformationen zu überprüfen oder Übertragungsanfragen zu autorisieren.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die Domains .com.au und .net.au sind offen für Partnerschaften oder Einzelfirmen, die in Australien registriert sind, ausländische Unternehmen mit Handelslizenz in Australien; sowie Eigentümer oder Anmelder einer in Australien registrierten Handelsmarke. Einzelpersonen können keine .com.au/.net.au-Domains registrieren. Der Kontakt des Registranten muss ein Unternehmen sein.
- Ihr Domainname muss identisch mit Ihrem Namen (wie bei den entsprechenden australischen Behörden registriert) oder mit Ihrer Marke (oder der Abkürzung bzw. dem Akronym für Ihre Marke) sein.
- Der Domainname muss auf Ihre Aktivität hinweisen. Beispielsweise sollte er ein Produkt angeben, das Sie verkaufen, oder eine Dienstleistung, die Sie bereitstellen.
- Während des Registrierungsvorgangs müssen Sie folgende Informationen angeben:
  - Ihr Registrierungstyp: ABN (australische Geschäftsnummer), ACN (australische Firmennummer) oder TM (Marke), wenn der Domainname Ihrer Marke entspricht.
  - Ihre ID-Nummer, die eine ABN (australische Geschäftsnummer), ACN (australische Firmennummer) oder TM (Marke) sein kann, wenn der Domainname Ihrer Marke entspricht.
  - Ihr Registrantenname, der der Name der juristischen Person ist, die die Domain registriert. Dieser Wert muss genau mit dem Namen auf dem angegebenen Namen übereinstimmen.
  - Ihr Berechtigungstyp, der sich auf die Art der juristischen Person bezieht, die diesen Domainnamen registriert.
  - Der Grund, warum Sie diesen Domainnamen registrieren dürfen (politischer Grund):
    - Der Domainname entspricht dem Akronym oder der Abkürzung des Unternehmens- oder Handelsnamens, des Organisations- oder Verbandsnamens oder der Marke des Registranten. (Politischer Grund 1)
    - Der Domainname entspricht den Zuteilungsregeln, ist jedoch kein Akronym oder eine Abkürzung für den Firmen- oder Handelsnamen, den Organisations- oder Verbandsnamen oder die Marke des Registranten. (Politischer Grund 2). Die Zuteilungsregeln für .com.au finden Sie in SCHEDULE C in der Registrierung .com.au.

- Falsche oder nicht übereinstimmende Kontaktinformationen, einschließlich Name, ABN oder Markennummer (TM), führen zu Fehlern bei der Registrierung, beim Handel und bei Verlängerungen. Möglicherweise ist eine Eigentümeränderung erforderlich, um Informationen für vorhandene Domains zu korrigieren.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Wenn Sie den Schlüssel festlegen, müssen Sie den DNS-Sicherheitsalgorithmus 2 (DH) wählen. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 60 Tagen vor Ablauf und dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 29 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 30 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .com.au-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten,

bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

Ändern der Eigentümerschaft

Ändern Sie den Besitzer, entweder programmgesteuert oder über die Route-53-Konsole. Siehe Aktualisieren der Kontaktinformationen für eine Domäne. Führen Sie dann den folgenden Vorgang ab, um die Besitzeränderung abzuschließen:

1. Sowohl der alte als auch der neue Registrant müssen auf den Link klicken, den sie in einer E-Mail von transfers@1api.net an ihre angegebenen E-Mail-Adressen erhalten. Wenn dies nicht innerhalb von 14 Tagen abgeschlossen ist, müssen Sie den Vorgang erneut starten.

2. Nachdem die Antworten bestätigt wurden, wird die Besitzeränderung in der Registrierung in kurzer Zeit ohne weitere Bestätigung bearbeitet.

.com.sg (Republik Singapur)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .com.sg-Domains zu registrieren oder .com.sg-Domains an Route 53 zu übertragen. Die .com.sg-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Ein oder zwei Jahre.

Löschen der Domainregistrierung

Die Registrierungsstelle für .com.sg-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .com.sg-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 60 Tage nach Ablauf

.fm (Föderierte Staaten von Mikronesien)

Wird auch als generische TLD verwendet, häufig von Unternehmen im Zusammenhang mit Online-Medien und Rundfunk.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 44 Tagen und 79 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 84 Tage nach Ablauf

.in (Indien)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 65 Tage nach Ablauf

.jp (Japan)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einer Einschränkung:

- Nur Einzelpersonen oder Unternehmen in Japan können einen .jp-Domainnamen registrieren.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt für Japanisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Eine Verlängerung ist möglich: Bis 16 Tage vor dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: 6 Tage vor Ablauf
- Wiederherstellung mit der Registrierung möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

> **Note**
>
> Die Registrierung von non-general-purpose JP-Domains wie .co.jp und .or.jp ist derzeit nicht möglich.

.io (Britisches Territorium im Indischen Ozean)

Wird auch als generische TLD verwendet, oftmals von IT-Organisationen wie Online-Services, Browser-basierten Spielen und Startup-Unternehmen.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Alle Informationen außer state/province dem Land sind versteckt.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

Die Registrierung für. io Domains verwendet auch den Autorisierungscode als Kennwort zur einmaligen Verwendung für manche Vorgänge, etwa die Aktivierung oder Deaktivierung des Datenschutzes. Wenn Sie mehr als einen kennwortpflichtigen Vorgang ausführen möchten, müssen Sie für jeden Vorgang einen weiteren Autorisierungscode erstellen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Die Domain wird aus der Registrierung gelöscht: 90 Tage nach Ablauf

.net.au (Australien)

Return to index

Bestätigungs-E-Mail von der TLD-Registrierungsstelle

Unser Registrar-Mitarbeiter, Gandi, verkauft .net.au-Domains weiter über. DomainDirectors Wenn Sie einen Domainnamen auf Route 53 übertragen, DomainDirectors sendet er eine E-Mail an den Ansprechpartner des Registranten für die Domain, um die Kontaktinformationen zu überprüfen oder Übertragungsanfragen zu autorisieren.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die Domains .com.au und .net.au sind offen für juristische Personen, Handelsunternehmen, Partnerschaften oder Einzelfirmen, die in Australien registriert sind, ausländische Unternehmen mit Handelslizenz in Australien; sowie Eigentümer oder Anmelder einer in Australien registrierten Handelsmarke.
- Ihr Domainname muss identisch mit Ihrem Namen (wie bei den entsprechenden australischen Behörden registriert) oder mit Ihrer Marke (oder der Abkürzung bzw. dem Akronym für Ihre Marke) sein.
- Der Domainname muss auf Ihre Aktivität hinweisen. Beispielsweise sollte er ein Produkt angeben, das Sie verkaufen, oder eine Dienstleistung, die Sie bereitstellen.
- Während des Registrierungsvorgangs müssen Sie Folgendes angeben:
  - Ihr Registrierungstyp: ABN (australische Geschäftsnummer), ACN (australische Firmennummer) oder TM (Marke), wenn der Domainname Ihrer Marke entspricht.
  - Ihre ID-Nummer, die eine ABN (australische Geschäftsnummer), ACN (australische Firmennummer) oder TM (Marke) sein kann, wenn der Domainname Ihrer Marke entspricht.
  - Ihr Registrantenname, der der Name der juristischen Person ist, die die Domain registriert. Dieser Wert muss genau mit dem Namen auf dem angegebenen Namen übereinstimmen.
  - Ihr Berechtigungstyp, der sich auf die Art der juristischen Person bezieht, die diesen Domainnamen registriert.
  - Der Grund, warum Sie diesen Domainnamen registrieren dürfen (politischer Grund):
    - Der Domainname entspricht dem Akronym oder der Abkürzung des Unternehmens- oder Handelsnamens, des Organisations- oder Verbandsnamens oder der Marke des Registranten. (Politischer Grund 1)
    - Der Domainname entspricht den Zuteilungsregeln, ist jedoch kein Akronym oder eine Abkürzung für den Firmen- oder Handelsnamen, den Organisations- oder Verbandsnamen oder die Marke des Registranten. (Politischer Grund 2). Die Zuweisungsregeln für .net.au finden Sie in SCHEDULE E in der net.au-Registrierung.
- Falsche oder nicht übereinstimmende Kontaktinformationen, einschließlich Name, ABN oder Markennummer (TM), führen zu Fehlern bei der Registrierung, beim Handel und bei

Verlängerungen. Möglicherweise ist eine Eigentümeränderung erforderlich, um Informationen für vorhandene Domains zu korrigieren.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die API-Aktion einschränken. RetrieveDomainAuthCode (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Wenn Sie den Schlüssel festlegen, müssen Sie den DNS-Sicherheitsalgorithmus 2 (DH) wählen. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 60 Tagen vor Ablauf und dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 29 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 30 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .net.au-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

Ändern der Eigentümerschaft

Ändern Sie den Besitzer, entweder programmgesteuert oder über die Route-53-Konsole. Siehe Aktualisieren der Kontaktinformationen für eine Domäne. Führen Sie dann den folgenden Vorgang ab, um die Besitzeränderung abzuschließen:

1. Sowohl der alte als auch der neue Registrant müssen auf den Link klicken, den sie in einer E-Mail von transfers@1api.net an ihre angegebenen E-Mail-Adressen erhalten. Wenn dies nicht innerhalb von 14 Tagen abgeschlossen ist, müssen Sie den Vorgang erneut starten.

2. Nachdem die Antworten bestätigt wurden, wird die Besitzeränderung in der Registrierung in kurzer Zeit ohne weitere Bestätigung bearbeitet.

.net.nz (Neuseeland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen mindestens 18 Jahre alt sein.
- Organisationen müssen registriert sein.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: zwischen 44 und 134 Tagen nach Ablauf
- Löschung der Domain aus der Registrierung: 134 Tage nach Ablauf

.nz (Neuseeland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen mindestens 18 Jahre alt sein.
- Organisationen müssen registriert sein.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: zwischen 44 und 134 Tagen nach Ablauf
- Löschung der Domain aus der Registrierung: 134 Tage nach Ablauf

.org.nz (Neuseeland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen mindestens 18 Jahre alt sein.
- Organisationen müssen registriert sein.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und

anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 44 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: zwischen 44 und 134 Tagen nach Ablauf
- Löschung der Domain aus der Registrierung: 134 Tage nach Ablauf

.pw (Palau)

Return to index

Das .pw war ursprünglich den Bewohnern von Palau vorbehalten, einem Inselstaat in der Mikronesien Subregion Ozeaniens im westlichen Pazifik. Heute wird es jedoch häufig für „Professional Web“ verwendet und steht allen zur Verfügung.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.qa (Katar)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .qa-Domains zu registrieren oder .qa-Domains an Route 53 zu übertragen. Die .qa-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Ein bis fünf Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .qa-Domains mehr in Route 53 übertragen.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 31 Tage nach Ablauf

.ru (Russische Föderation)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .ru-Domains zu registrieren oder .ru-Domains an Route 53 zu übertragen. Die .ru-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

> **Note**
>
> Die Registrierungsstelle für.ru-Domains aktualisiert das Ablaufdatum für eine Domain an dem Tag, an dem die Domain abläuft. WHOIS-Abfragen zeigen das alte Ablaufdatum für die Domain. Dabei spielt es keine Rolle, wann Sie die Domain mit Route 53 erneuern.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen möglicherweise eine Passnummer oder eine von einer Behörde ausgestellte ID-Nummer angeben.
- Ausländische Unternehmen benötigen eine Unternehmens-ID oder Handelsregisternummer.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .ru-Domains mehr in Route 53 übertragen.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu 2 Tage vor dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: 2 Tage vor Ablauf

- Wiederherstellung mit der Registrierung möglich: Zwischen 2 Tagen vor und 28 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 28 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .ru-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.sg (Republik Singapur)

> **Important**
>
> Sie können Route 53 nicht mehr verwenden, um neue .sg-Domains zu registrieren oder .sg-Domains an Route 53 zu übertragen. Die .sg-Domains, die bereits bei Route 53 registriert sind, werden weiter unterstützt.

Return to index

Verlängerungszeitraum

Ein oder zwei Jahre.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Nicht unterstützt Sie können keine .sg-Domains mehr in Route 53 übertragen.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 60 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .sg-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

Europa

Sie können die folgenden Top-Level-Domains (TLDs) für Europa verwenden, um Domains bei Amazon Route 53 zu registrieren.

, , , , , , , , , , , , , , , , , , ,

Return to index

.be (Belgien)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja. Den Transfercode erhalten Sie auf der Website von DNS Belgien.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: Am Ablaufdatum
- Wiederherstellung mit der Registrierung möglich: Bis zu 40 Tage nach Ablauf
- Domain wird aus der Registrierung gelöscht: 40 Tage nach Ablauf

.berlin (Stadt Berlin, Deutschland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Der Eigentümer, der administrative oder technische Ansprechpartner muss eine Adresse in Berlin haben, und der administrative Kontakt muss eine Einzelperson sein.
- Sie müssen Ihre .berlin-Domain innerhalb von 12 Monaten nach der Registrierung aktivieren und verwenden (gilt für eine Website, Umleitung oder E-Mail-Adresse).
- Wenn Sie eine Website unter der Domain .berlin veröffentlichen oder wenn .berlin auf eine andere Website umleitet, muss der Inhalt der Website im Zusammenhang mit Berlin stehen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Latein und Kyrillisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 80 Tage nach Ablauf

.ch (Schweiz)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 9 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 9 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 9 Tagen und 49 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 49 Tage nach Ablauf

.co.uk (Großbritannien und Nordirland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Wenn Sie eine .co.uk-Domain zu Route 53 übertragen, müssen Sie keinen Autorisierungscode abrufen. Verwenden Sie stattdessen die von Ihrer aktuellen Domains-Vergabestelle angegebene Methode, um den Wert des IPS-Tags für die Domain auf GANDI zu aktualisieren, komplett in Großbuchstaben. (Ein IPS-Tag ist für Nominet erforderlich, der Registrierungsstelle für .uk-Domainnamen.) Wenn Ihre Vergabestelle den Wert des IPS-Tag nicht ändert, wenden Sie sich bitte an Nominet.

> **Note**
>
> Wenn Sie eine .co.uk-Domain registrieren, legt Route 53 automatisch das IPS-Tag für die Domain auf GANDI fest.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 180 Tagen vor und 30 Tagen nach dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Zwischen 30 Tagen und 90 Tagen nach Ablauf
- Domain wird aus Route 53: gelöscht: 90 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 92 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .co.uk-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.cz (Tschechische Republik)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt, aber E-Mail-Adresse und Telefonnummer werden für alle Kontakte ausgeblendet.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

Wenn Ihre derzeitige Vergabestelle keinen Autorisierungscode angibt, gehen Sie zu `https://www.nic.cz/whois/send-password/`, um anzufordern, dass er von der CZ-Domainregistrierungsstelle an die E-Mail-Adresse des Registranten gesendet wird.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 58 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 59 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 60 Tage nach Ablauf

.de (Deutschland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Sie müssen in Deutschland wohnen oder über einen administrativen Kontakt (natürliche Person) verfügen, die in Deutschland ihren Wohnsitz und eine Adresse hat (kein Postfach).
- Während der Registrierung muss der DNS-Name (A, MX und CNAME) des Domainnamens korrekt konfiguriert sein, damit er die Zonenprüfung der Registrierungsstelle besteht. Drei Server aus zwei verschiedenen C-Klassen sind erforderlich.
- Wenn Sie einen anderen DNS-Service als Route 53 verwenden, müssen die Namenserver für die Domain eine Überprüfung bestehen, um sicherzustellen, dass sie korrekt konfiguriert sind. Um festzustellen, ob die Nameserver für Ihre Domain die Prüfung bestehen, besuchen Sie https://www.denic. de/en/service/tools/nast/.
- Sie müssen Kontaktinformationen angeben, die den Anforderungen zur Überprüfung der Registrierung entsprechen. Ungültige oder falsch formatierte Kontaktdaten können dazu führen, dass Domainverlängerungen fehlschlagen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: Am Ablaufdatum
- Wiederherstellung mit der Registrierung möglich: Wenden Sie sich an AWS -Support.
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

.es (Spanien)

Return to index

Domainkauf oder -übertragung

> **Important**
>
> Derzeit können Sie neue .es-Domainnamen kaufen oder .es-Domains auf Route 53 übertragen. Der Kontakttyp für den Kontakt mit dem Registranten unterliegt keinen Einschränkungen. Der Kontakttyp Admin/Tech/Billing muss eine Person sein.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, für alle, die in Verbindung mit Spanien stehen oder Interesse daran haben.

Seit 2016 müssen die Registranten der .ES-Domain eine Kontakt-E-Mail angeben. Wenn Sie diese Informationen nicht angegeben haben, müssen Sie dies bei Ihrer derzeitigen Vergabestelle nachholen, bevor Sie Ihre Domain zu Route 53 übertragen.

Sie benötigen die folgenden Informationen:

- ESNIC-Kennung ähnlich *AAAA0-ESNIC-F0* wie.
- Wenn Sie Ihre ESNIC-ID nicht kennen, können Sie sie von der aktuellen Vergabestelle erfahren. Sie finden Ihre Vergabestelle unter: https://www.dominios.es/en.

Je nachdem, ob Sie sich an Ihr Passwort bei der Vergabestelle erinnern oder nicht, können Sie eines der folgenden Verfahren anwenden, um Ihre Registrant-E-Mail zu aktualisieren:

- Wenn Sie sich an Ihr Passwort erinnern, melden Sie sich unter https://www.nic an. es/sgnd/login.action, indem Sie Ihre ESNIC-IDs und Ihr Passwort verwenden.

  Nachdem Sie sich angemeldet haben, können Sie den E-Mail-Kontakt des Registranten bearbeiten, indem Sie auf der Registrierungsseite die Registerkarte Bearbeiten wählen.
- Wenn Sie Ihr Passwort vergessen haben, gehen Sie zu https://www.nic. es/sgnd/peticion/editCorreo.aktion? request_locale=de.

  Füllen Sie das Formular mit Ihrer ESNIC-ID, Ihrem neuen und gültigen E-Mail-Kontakt als Registrant aus. Validieren Sie dann das Formular, indem Sie Verarbeiten ohne eID/Zertifikat wählen, und laden Sie das angeforderte Ausweisdokument hoch.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

Die .es-Registrierung verwaltet den Autorisierungscode mit einem time-to-live und er kann ablaufen. Sie können den Authentifizierungscode aktualisieren, indem Sie den Status der Transfersperre (clientTransferProhibited) von Ihrer Domain entfernen, falls er vorhanden ist. Wenn die Domain keine Übertragungssperre hat, können Sie den Authentifizierungscode aktualisieren, indem Sie ihn zuerst ein- und dann ausschalten.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu 6 Tage vor dem Ablaufdatum

- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: 6 Tage vor Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 6 Tagen vor und 4 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 4 Tage nach Ablauf

.eu (Europäische Union)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einer Einschränkung:

- Sie müssen eine gültige Postanschrift aus einer der 30 Staaten des Europäischen Wirtschaftsraums (EWR) angeben, oder wenn Sie Bürger einer der 27 Mitgliedstaaten der Europäischen Union (EU) sind, müssen Sie Ihr EU-Bürgerland angeben.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

Sie können den Authentifizierungscode auch mithilfe des Fensters „My.eu“ in der Registrierung generieren: https://my.eurid.eu/.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: Am Ablaufdatum
- Wiederherstellung mit der Registrierung möglich: Bis zu 40 Tage nach Ablauf
- Domain wird aus der Registrierung gelöscht: 40 Tage nach Ablauf

WHOIS-Abfragen

Weitere Informationen zu vorhandenen .eu-Domains finden Sie unter https://whois.eurid.eu/en/.

.fi (Finnland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis fünf Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Die .fi-Erweiterung ist für Personen verfügbar, die ihren Wohnsitz in Finnland haben und über eine Finnisch ID-Nummer verfügen, sowie für juristische Personen oder private Unternehmer, die in Finnland registriert sind.
- Wenn sich die Kontaktadresse des Registranten in Finnland befindet, ist für einen einzelnen Registranten eine finnische Identitätsnummer und für einen Unternehmensregistranten eine finnische Unternehmensnummer erforderlich, und Sie müssen bei der Registrierung die folgenden Informationen angeben:
  - Angabe, ob der Kontakt auf einer natürlichen oder juristischen Person in Finnland basiert.
  - Die ID der Registrierung, wo der Name aufgezeichnet ist, wenn er auf einer juristischen Person basiert.
  - Die Nummer des Eintrags in der Registrierung, wo der Name aufgezeichnet ist, wenn er auf einer juristischen Person basiert.

- Die Identifikationsnummer für eine juristische Person in Finnland.
- Die Identifikationsnummer für eine natürliche Person in Finnland.
- Wenn es sich bei dem Registranten um ein nicht finnisches Unternehmen handelt, müssen Sie die Geschäftsnummer als Umsatzsteuer-Identifikationsnummer angeben.

- Wenn sich die Adresse des Registranten nicht in Finnland befindet, ist keine finnische Identitäts- oder Unternehmensnummer erforderlich.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die API-Aktion einschränken. RetrieveDomainAuthCode (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: Nein

Löschen der Domainregistrierung

Weitere Informationen zum Löschen einer Domain finden Sie unter Löschen einer Domainnamen-Registrierung.

.fr (Frankreich)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Personen müssen mindestens 18 Jahre alt sein und ihre angebendate-of-birth.
- Organisationen müssen sich im europäischen Wirtschaftsraum oder in der Schweiz befinden.
- Unternehmen sollten alle Felder zur Unternehmensidentifikation ausfüllen (USt, SIREN, WALDEC, DUNS usw.), da dies die Überprüfung erleichtert, die AFNIC möglicherweise zu einem späteren Zeitpunkt durchführt.
- Die gleichen Voraussetzungen gelten für den administrativen Kontakt.
- Names und Bezeichnungen unterliegen einer vorherigen Überprüfung durch AFNIC (Namens-Charta Artikel 2.4) und den folgenden zusätzlichen Bedingungen:
  - Zuvor reservierte oder verbotene Domainnamen sind für Antragsteller verfügbar, die ein legitimes Recht nachweisen und in gutem Glauben handeln.
  - Namen, die mit ville, mairie, agglo, cc, cg und cr beginnen, unterliegen der AFNIC-Namenskonvention.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Überweisungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 27 Tage nach Ablauf
- Domain wird aus Route 53 gelöscht: 28 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 28 Tagen und 58 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 58 Tage nach Ablauf

.gg (Guernsey)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 35 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 35 Tage nach Ablauf

.im (Isle of Man)

Auch als generische TLD verwendet, häufig durch Instant Messaging-Services oder von Personen, die eine persönliche "Ich bin"-Marke entwickeln möchten.

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein oder zwei Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf

- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 30 Tage nach Ablauf

.it (Italien)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Einzelpersonen oder Organisationen müssen über eine registrierte Adresse in der Europäischen Union verfügen.
- Wenn Ihr Herkunftsland Italien ist, müssen Sie einen Steuercode eingeben. Wenn Ihr Herkunftsland innerhalb der Europäischen Union liegt, müssen Sie eine Identitätsdokumentnummer (ID-Nummer) eingeben.
- Namensserver für Ihre Domain müssen eine DNS-Prüfung bestehen. Wir empfehlen Ihnen, die Nameserver unter https://dns-check.nic.it/, bevor Sie den Änderungsantrag einreichen. Entspricht Ihr Domainname nicht den technischen Voraussetzungen (z. B. ist er keinem funktionsfähigen Nameserver zugeordnet) und korrigieren Sie ihn nicht innerhalb von 30 Tagen, wird Ihr Domainname von der Registry gelöscht. Es gibt keine Erstattungen für Domains, die gelöscht werden, weil sie nicht den technischen Anforderungen entsprechen.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 13 Tage nach Ablauf
- Domain wird aus der Registrierung gelöscht: 49 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 14 Tagen und 44 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

.me (Montenegro)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Domain.me, die Registrierungsstelle für .me-Domains, betrachtet aus zwei Buchstaben bestehende Domainnamen und einige längere Domainnamen als Premium-Domainnamen. Sie können keine Premium-.me-Domains in Route 53 registrieren oder übertragen. Weitere Informationen über Premium-.me-Domainnamen finden Sie auf der Website domain.me.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Arabisch, Weißrussisch, Bosnisch, Bulgarisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Kroatisch, Dänisch, Französisch, Deutsch, Hindi, Ungarisch, Isländisch,

Italienisch, Koreanisch, Lettisch, Litauisch, Mongolisch, Montenegrin, Polnisch, Portugiesisch, Russisch, Serbisch, Spanisch, Schwedisch, Türkisch und Ukrainisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 29 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 30 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 30 Tagen und 60 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 65 Tage nach Ablauf

.me.uk (Großbritannien und Nordirland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Wenn Sie eine .me.uk-Domain zu Route 53 übertragen, müssen Sie keinen Autorisierungscode abrufen. Verwenden Sie stattdessen die von Ihrer aktuellen Domains-Vergabestelle angegebene Methode, um den Wert des IPS-Tags für die Domain auf GANDI zu aktualisieren, komplett in Großbuchstaben. (Ein IPS-Tag ist für Nominet erforderlich, der Registrierungsstelle für .uk-Domainnamen.) Wenn Ihre Vergabestelle den Wert des IPS-Tag nicht ändert, wenden Sie sich bitte an Nominet.

> **Note**
>
> Wenn Sie eine .me.uk-Domain registrieren, legt Route 53 automatisch das IPS-Tag für die Domain auf GANDI fest.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 180 Tagen vor und 30 Tagen nach dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Zwischen 30 Tagen und 90 Tagen nach Ablauf
- Domain wird aus Route 53: gelöscht: 90 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 92 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .me.uk-Domain lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.nl (Niederlande)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein Jahr.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Der Eigentümer oder der administrativen Kontakt muss eine gültige Adresse in den Niederlanden haben. Eine Vor-Ort-Präsenz ist erforderlich.
- Wenn Sie nicht über eine gültige Adresse in den Niederlanden verfügen, stellt Ihnen die Registrierungsstelle SIDN eine Wohnsitzadresse gemäß Domicile Address Procedure zur Verfügung.
- Der Domainname muss 3-63 Zeichen lang sein, ausgenommen .nl.

Datenschutz

Abhängig von der Registrierungsstelle.

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu 1 Tag vor dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein

- Domain wird aus Route 53 gelöscht: 1 Tag vor Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 1 Tag vor und 39 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 39 Tage nach Ablauf

.org.uk (Großbritannien und Nordirland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Wenn Sie eine .org.uk-Domain zu Route 53 übertragen, müssen Sie keinen Autorisierungscode abrufen. Verwenden Sie stattdessen die von Ihrer aktuellen Domains-Vergabestelle angegebene Methode, um den Wert des IPS-Tags für die Domain auf GANDI zu aktualisieren, komplett in Großbuchstaben. (Ein IPS-Tag ist für Nominet erforderlich, der Registrierungsstelle für .uk-Domainnamen.) Wenn Ihre Vergabestelle den Wert des IPS-Tag nicht ändert, wenden Sie sich bitte an Nominet.

> **Note**
>
> Wenn Sie eine .org.uk-Domain registrieren, legt Route 53 automatisch das IPS-Tag für die Domain auf GANDI fest.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 180 Tagen vor und 30 Tagen nach dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Zwischen 30 Tagen und 90 Tagen nach Ablauf
- Domain wird aus Route 53: gelöscht: 90 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 92 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .org.uk-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.ruhr (Ruhrgebiet, Westdeutschland)

Return to index

Die Erweiterung .ruhr gilt für das Ruhrgebiet im Westen Deutschlands.

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einer Einschränkung:

- Der administrative Kontakt muss eine Person mit einer Adresse in Deutschland sein.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt (ä, ö, ü, ß).

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: Wenden Sie sich an AWS -Support.

.se (Schweden)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Wenn Sie sich in Schweden befinden, müssen Sie eine gültige schwedische ID-Nummer haben. Das Format der ID-Nummer lautet`YYMMDD-NNNN`.
- Wenn Sie sich außerhalb von Schweden befinden, müssen Sie eine gültige ID-Nummer eingeben, z. B. die Steuer-ID-Nummer.

Zusätzliche Überprüfungsanforderungen

Ab dem 1. Oktober 2025 erfordern Registrierungen von.se-Domains eine zusätzliche Identitätsprüfung, um die neuen NIS 2.0-Anforderungen der Registry zu erfüllen. Wenn Sie

eine.se-Domain registrieren, setzen wir uns mit Ihnen in Verbindung, um Bestätigungsdokumente anzufordern. Ihre Domainregistrierung bleibt solange ausstehend, bis Sie die erforderlichen Dokumente vorgelegt haben und die Überprüfung abgeschlossen ist. Um Ihre Dokumente einzureichen, wenden Sie sich an den AWS Support.

Die.se-Registry führt auch regelmäßige Prüfungen vorhandener Domains durch und fordert möglicherweise zusätzliche Verifizierungen für kürzlich registrierte Domains an oder wenn Sie bestimmte Änderungen an Ihrer Domain vornehmen (z. B. die Aktualisierung des Domaininhabers oder der Kontaktinformationen). Wenn Ihre Domain in `serverHold` den Status versetzt wird, bedeutet dies, dass die Registrierung eine Überprüfung erfordert, bevor Ihre Domain vollständig aktiviert werden kann.

Dokumente, die Sie bereitstellen müssen:

- Für Einzelpersonen: Ein von der Regierung ausgestelltes Ausweisdokument (z. B. ein Personalausweis oder Reisepass) und ein Adressnachweis, der weniger als 3 Monate alt ist.
- Für Unternehmen oder Organisationen: Registrierungsbescheinigung des Unternehmens oder der Organisation und Adressnachweis, falls dieser von der Registrierungsbescheinigung abweicht.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen Ihnen, unbefugte Übertragungen zu verhindern, indem Sie den Zugriff auf die RetrieveDomainAuthCodeAPI-Aktion einschränken. (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole und anderer programmatischer Methoden einen Autorisierungscode generieren kann.) AWS SDKs Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt für Latein, Schwedisch und Jiddisch.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zu 1 Tag vor dem Ablaufdatum
- Späte Erneuerung mit Route 53 möglich: Nein
- Domain wird aus Route 53 gelöscht: 1 Tag vor Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 1 Tag vor und 59 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 64 Tage nach Ablauf

.uk (Großbritannien und Nordirland)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, ohne Einschränkungen.

Datenschutz

Alle Informationen sind verborgen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt

Internationalisierte Domainnamen

Nicht unterstützt

Für Übertragungen ist ein Autorisierungscode erforderlich

Wenn Sie eine uk-Domain zu Route 53 übertragen, müssen Sie keinen Autorisierungscode angeben. Verwenden Sie stattdessen die von Ihrer aktuellen Domains-Vergabestelle angegebene Methode, um den Wert des IPS-Tags für die Domain auf GANDI zu aktualisieren, komplett in Großbuchstaben. (Ein IPS-Tag ist für Nominet erforderlich, der Registrierungsstelle für .uk-Domainnamen.) Wenn Ihre Vergabestelle den Wert des IPS-Tag nicht ändert, wenden Sie sich bitte an Nominet.

> **Note**
>
> Wenn Sie eine .uk-Domain registrieren, legt Route 53 automatisch das IPS-Tag für die Domain auf GANDI fest.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 180 Tagen vor und 30 Tagen nach dem Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Zwischen 30 Tagen und 90 Tagen nach Ablauf
- Domain wird aus Route 53: gelöscht: 90 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Nein
- Domain wird aus der Registrierung gelöscht: 92 Tage nach Ablauf

Löschen der Domainregistrierung

Die Registrierungsstelle für .uk-Domains lässt das Löschen von Domainregistrierungen nicht zu. Stattdessen müssen Sie die automatische Verlängerung deaktivieren und warten, bis die Domain abläuft. Weitere Informationen finden Sie unter Löschen einer Domainnamen-Registrierung.

.wien (Stadt Wien, Österreich)

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Einschränkungen

Für die Öffentlichkeit nutzbar, mit einigen Einschränkungen:

- Sie müssen eine wirtschaftliche, kulturelle, touristische, historische, soziale oder andere Verbundenheit mit der Stadt Wien in Österreich nachweisen.
- Die .wien-Domainnamen müssen für die Laufzeit der Registrierung unter Berücksichtigung der zuvor genannten Bedingungen verwendet werden.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt für Latein.

Für Übertragungen ist ein Autorisierungscode erforderlich

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 80 Tage nach Ablauf

Konfigurieren von Amazon Route 53 als DNS-Service

Sie können Route 53 als DNS-Service für Ihre Domäne verwenden, z. B. "example.com". Wenn Route 53 Ihr DNS-Service ist, leitet dieser Internetdatenverkehr an Ihre Website weiter, indem er benutzerfreundliche Domänennamen wie www.beispiel.de in numerische IP-Adressen wie 192.0.2.1 übersetzt, die zur Verbindung zwischen Computern verwendet werden. Wenn ein Benutzer Ihren Domänennamen in einen Browser eingibt oder Ihnen eine E-Mail sendet, wird eine DNS-Abfrage an Route 53 weitergeleitet und daraufhin mit dem entsprechenden Wert beantwortet. Beispielsweise könnte Route 53 mit der IP-Adresse für den Web-Server für example.com antworten.

> **⚠ DNS-Hosting im Vergleich zur Domainregistrierung**
>
> In diesem Kapitel wird nur die Verwendung von Route 53 für DNS-Hosting behandelt. Das bedeutet, dass Ihre Domainregistrierung bei Ihrem derzeitigen Registrar verbleibt und Sie ihn weiterhin für Domainverlängerungen bezahlen müssen. Route 53 verwaltet nur Ihre DNS-Einstellungen und bearbeitet DNS-Abfragen für Ihre Domain.
>
> Wenn Sie Ihre Domainregistrierung auch auf Route 53 übertragen möchten (sodass Route 53 sowohl Ihr Registrar als auch Ihr DNS-Dienst ist), finden Sie weitere Informationen unter Checkliste vor der Übertragung für Domainübertragungen undÜbertragen der Registrierung für eine Domain an Amazon Route 53.

In diesem Abschnitt wird erläutert, wie Sie Route 53 so konfigurieren, dass Ihr Internetdatenverkehr korrekt weitergeleitet wird. Außerdem wird erläutert, wie Sie einen DNS-Service zu Route 53 migrieren, wenn Sie aktuell einen anderen DNS-Service nutzen, und wie Sie Route 53 als DNS-Service für eine neue Domäne verwenden.

Themen

- DNS-Einschränkungen und Verhaltensweisen
- Verwandte Themen

Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen

Wenn Sie eine oder mehrere Domänenregistrierungen zu Route 53 übertragen und Sie derzeit eine Domänenvergabestelle verwenden, die keinen kostenpflichtigen DNS-Dienst anbietet, müssen Sie vor dem Migrieren der Domäne zuerst den DNS-Dienst migrieren. Andernfalls bietet die Vergabestelle keinen DNS-Dienst mehr an, wenn Sie Ihre Domänen übertragen, und die verknüpften Websites und Webanwendungen sind im Internet nicht mehr verfügbar. (Sie können auch den DNS-Dienst von der aktuellen Vergabestelle zu einem anderen DNS-Dienstanbieter migrieren. Es ist nicht erforderlich, dass Sie Route 53 als DNS-Dienstanbieter für Domänen verwenden, die bei Route 53 registriert sind.)

Der Prozess hängt davon ab, ob Sie die Domäne derzeit nutzen:

- Wenn die Domäne derzeit Datenverkehr erhält, zum Beispiel, wenn Ihre Benutzer den Domänennamen verwenden, um eine Website zu suchen oder auf eine Webanwendung zuzugreifen, finden Sie weitere Informationen unter Route 53 als DNS-Dienst für eine Domäne nutzen, die in Gebrauch ist.
- Wenn die Domäne keinen (oder nur sehr wenig) Datenverkehr erhält, finden Sie weitere Informationen unter Route 53 als DNS-Dienst für eine inaktive Domäne nutzen.

Bei beiden Optionen bleibt Ihre Domäne während des gesamten Migrationsprozesses verfügbar. In dem unwahrscheinlichen Fall, dass Probleme auftreten, können Sie die Migration mit der ersten Option schnell zurücksetzen. Mit der zweiten Option ist Ihre Domäne möglicherweise einige Tage nicht verfügbar.

Wenn Sie sich mit einem Experten unter in Verbindung setzen möchten AWS, besuchen Sie den Vertriebssupport.

Route 53 als DNS-Dienst für eine Domäne nutzen, die in Gebrauch ist

Wenn Sie den DNS-Dienst zu Amazon Route 53 für eine Domäne migrieren möchten, die derzeit Datenverkehr erhält, z. B. wenn Ihre Benutzer den Domänennamen verwenden, um eine Website zu finden oder auf eine Webanwendung zuzugreifen, führen Sie die Schritte in diesem Abschnitt aus.

Themen

Schritt 1: Abrufen Ihrer aktuellen DNS-Konfiguration vom aktuellen DNS-Dienstanbieter (optional, jedoch empfohlen)

Wenn Sie einen DNS-Dienst von einem anderen Anbieter zu Route 53 migrieren, reproduzieren Sie Ihre aktuelle DNS-Konfiguration in Route 53. Erstellen Sie in Route 53 erst eine gehostete Zone mit demselben Namen wie Ihre Domäne und dann Datensätze in dieser gehosteten Zone. Jeder Datensatz gibt an, wie der Datenverkehr für einen bestimmten Domänen- oder Subdomänennamen weitergeleitet werden soll. Wenn beispielsweise jemand Ihren Domainnamen in einen Webbrowser eingibt, möchten Sie, dass der Datenverkehr an einen Webserver in Ihrem Rechenzentrum, an eine EC2 Amazon-Instance, an eine CloudFront Distribution oder an einen anderen Ort weitergeleitet wird?

Der Prozess, den Sie verwenden, hängt von der Komplexität Ihrer aktuellen DNS-Konfiguration ab:

- Wenn Ihre aktuelle DNS-Konfiguration einfach ist - Wenn Sie den Internetdatenverkehr nur für einige Subdomänen an eine geringe Anzahl von Ressourcen, wie Webserver oder Amazon-S3-Buckets, weiterleiten, können Sie einige Datensätze in der Route 53-Konsole manuell erstellen.
- Wenn Ihre aktuelle DNS-Konfiguration eher komplex ist und Sie Ihre aktuelle Konfiguration lediglich reproduzieren möchten - Sie können die Migration vereinfachen, wenn Sie eine Zonendatei vom

aktuellen DNS-Dienstanbieter abrufen können, und die Zonendatei in Route 53 importieren. (Nicht alle DNS-Dienstanbieter stellen Zonendateien zur Verfügung.) Beim Importieren einer Zonendatei reproduziert Route 53 die vorhandene Konfiguration automatisch, indem die entsprechenden Datensätze in Ihrer gehosteten Zone erstellt werden.

Fragen Sie beim Kundenservice Ihres aktuellen DNS-Dienstanbieters nach, wie Sie eine Zonendatei oder eine Datensatzliste erhalten. Informationen über das erforderliche Format der Zonendatei finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.

- Wenn Ihre aktuelle DNS-Konfiguration eher komplex ist und Sie an Route 53-Routing-Funktionen interessiert sind - Sehen Sie sich die folgende Dokumentation an, um festzustellen, ob Sie Route 53-Funktionen verwenden möchten, die von anderen DNS-Dienstanbietern nicht zur Verfügung gestellt werden. Wenn dies der Fall ist, können Sie entweder Datensätze manuell erstellen oder eine Zonendatei importieren und Datensätze zu einem späteren Zeitpunkt erstellen oder aktualisieren:
  - Wählen zwischen Alias- und Nicht-Alias-Datensätzenerklärt die Vorteile von Route 53-Aliasdatensätzen, die den Datenverkehr kostenlos an einige AWS Ressourcen wie CloudFront Distributionen und Amazon S3 S3-Buckets weiterleiten.
  - Auswählen einer Routing-Richtlinie erläutert die Route 53-Routing-Optionen, z. B. Routing basierend auf dem Standort Ihrer Benutzer, Routing auf Basis der Latenz zwischen Ihren Benutzern und Ressourcen, Routing basierend darauf, ob Ihre Ressourcen fehlerfrei sind, und Routing an Ressourcen basierend auf den von Ihnen angegebenen Gewichtungen.

> **Note**
>
> Sie können eine Zonendatei auch importieren und die Konfiguration zu einem späteren Zeitpunkt ändern, um Aliasdatensätze und komplexe Routing-Richtlinien zu nutzen.

Wenn Sie keine Zonendatei abrufen können oder Datensätze in Route 53 manuell erstellen möchten, müssen Sie wahrscheinlich u. a. folgende Datensätze migrieren:

- A (Address) -Datensätze — verknüpfen einen Domainnamen oder Subdomänennamen mit der IPv4 Adresse (z. B. 192.0.2.3) der entsprechenden Ressource
- AAAA-Einträge (Address) — verknüpfen einen Domainnamen oder Subdomainnamen mit der IPv6 Adresse (z. B. 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) der entsprechenden Ressource
- MX-Datensätze (Mail Server) - Datenverkehr an Mail-Server weiterleiten

- CNAME-Datensätze - Den Datenverkehr für einen Domänennamen (example.net) an einen anderen Domänennamen (example.com) weiterleiten
- Datensätze für andere unterstützte DNS-Datensatztypen - Eine Liste der unterstützen Datensatztypen finden Sie unter Unterstützte DNS-Datensatztypen.

Schritt 2: Erstellen einer gehosteten Zone

Um Amazon Route 53 mitzuteilen, wie Sie den Datenverkehr für Ihre Domäne weiterleiten möchten, erstellen Sie zuerst eine gehostete Zone mit demselben Namen wie Ihre Domäne und dann die Datensätze in der gehosteten Zone.

> **Important**
>
> Sie können eine gehostete Zone nur für eine Domäne erstellen, die Sie über die Berechtigung zur Verwaltung verfügen. Das heißt in der Regel, dass Sie Eigentümer der Domäne sind. Es könnte aber auch bedeuten, dass Sie eine Anwendung für den Eigentümer entwickeln.

Bei der Erstellung einer gehosteten Zone erstellt Route 53 automatisch einen NS-Eintrag (Namenserver) und einen SOA-Eintrag (Start of Authority, Autoritätsursprung) für die Zone. Der NS-Datensatz identifiziert die vier Namenserver, die Route 53 Ihrer gehosteten Zone zugeordnet hat. Um Route 53 als DNS-Dienst für Ihre Domäne festzulegen, aktualisieren Sie die Registrierung für die Domäne mit diesen vier Namenservern.

> **Important**
>
> Erstellen Sie keine zusätzlichen NS- (Namenserver) oder SOA-Datensätze (Autoritätsursprung) und löschen Sie die vorhandenen NS- und SOA-Datensätze nicht.

So erstellen Sie eine gehostete Zone

1. Melden Sie sich bei https://console.aws.amazon.com/route53/der an und öffnen AWS-Managementkonsole Sie die Route 53-Konsole unter.
2. Wenn Sie neu bei Route 53 sind, wählen SieMelden Sie sich in der &console; an und öffnen Sie die Seite &ConsolePageURL;.UNDERDNS-VerwaltungWählen Sie und anschließend ausGehostete Zonen erstellenaus.

Wenn Sie bereits Route 53 nutzen, wählen SieGehostete ZonenWählen Sie im Navigationsbereich und dannGehostete Zonen erstellenaus.

3. Geben Sie im Bereich Create Hosted Zone einen Domänennamen und optional einen Kommentar ein. Weitere Informationen zu einer Einstellung erhalten Sie, indem Sie das Hilfefenster auf der rechten Seite öffnen.

   Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

4. Übernehmen Sie für Type den Standardwert Public Hosted Zone.

5. Wählen Sie Create Hosted Zone.

Schritt 3: Erstellen von Datensätzen

Nachdem Sie eine gehostete Zone angelegt haben, erstellen Sie Datensätze in der gehosteten Zone, die definieren, wie Sie den Datenverkehr für eine Domäne (example.com) oder Subdomäne (www.example.com) weiterleiten möchten. Wenn Sie beispielsweise Traffic für example.com und www.example.com an einen Webserver auf einer EC2 Amazon-Instance weiterleiten möchten, erstellen Sie zwei Datensätze, einen mit dem Namen example.com und den anderen mit dem Namen www.example.com. In jedem Datensatz geben Sie die IP-Adresse für Ihre Instance an. EC2

Für das Erstellen von Datensätzen gibt es verschiedene Möglichkeiten:

Importieren einer Zonendatei

Dies ist die einfachste Methode, wenn Sie eine Zonendatei von Ihrem aktuellen DNS-Dienst in erhalten haben Schritt 1: Abrufen Ihrer aktuellen DNS-Konfiguration vom aktuellen DNS-Dienstanbieter (optional, jedoch empfohlen). Amazon Route 53 kann nicht vorhersagen, wann Aliasdatensätze erstellt oder spezielle Routing-Typen wie gewichtete oder Failover-Datensätze verwendet werden sollen. Daher erstellt Route 53 DNS-Standarddatensätze mithilfe der einfachen Routing-Richtlinie, wenn Sie eine Zonendatei importieren.

Weitere Informationen finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.

Erstellen von einzelnen DNS-Datensätzen in der Konsole

Wenn Sie keine Zonendatei erhalten haben und nur einige Datensätze mit der einfachen Routing-Richtlinie für die ersten Schritte erstellen möchten, können Sie die Datensätze in der Route 53 - Konsole erstellen. Sie können sowohl Alias- als auch Nicht-Alias-Datensätze erstellen.

Weitere Informationen finden Sie unter den folgenden Themen:

- Auswählen einer Routing-Richtlinie
- Wählen zwischen Alias- und Nicht-Alias-Datensätzen
- Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole

Programmgesteuertes Erstellen von Datensätzen

Sie können Datensätze erstellen, indem Sie einen der Befehle AWS SDKs AWS CLI, den oder verwenden AWS Tools for Windows PowerShell. Weitere Informationen finden Sie in der AWS Dokumentation.

Wenn Sie eine Programmiersprache verwenden, für die AWS kein SDK bereitgestellt wird, können Sie auch die Route 53-API verwenden. Weitere Informationen finden Sie unter Amazon Route 53 API Reference.

Schritt 4: Senken der TTL-Einstellungen

Die TTL-Einstellung (Time-to-live, Gültigkeitsdauer) für einen Datensatz gibt an, wie lange DNS-Resolver den Datensatz zwischenspeichern und die zwischengespeicherten Informationen verwenden sollen. Wenn die TTL abgelaufen ist, sendet ein Resolver eine weitere Abfrage an den DNS-Dienstanbieter für eine Domäne, um die neuesten Informationen zu erhalten.

Die typische TTL-Einstellung für den NS Datensatz ist 172 800 Sekunden oder 2 Tage. Der NS-Datensatz listet die Namenserver auf, die das Domain Name System (DNS) verwenden kann, um Informationen zum Weiterleiten des Datenverkehrs für Ihre Domäne abzurufen. Durch Senken der TTL für den NS-Datensatz sowohl für Ihren aktuellen DNS-Dienstanbieter als auch Amazon Route 53 werden die Ausfallzeiten für Ihre Domäne reduziert, wenn Sie beim Migrieren von DNS zu Route 53 ein Problem feststellen. Wenn Sie die TTL nicht senken, ist Ihre Domäne bis zu zwei Tage im Internet nicht verfügbar, wenn ein Fehler auftritt.

> **Note**
>
> Einige Vollresolver können die TTL des NS-Datensatzes des übergeordneten autoritativen Servers zwischenspeichern. Daher muss auch die TTL der auf dem übergeordneten autoritativen DNS-Server registrierten NS-Datensätze reduziert werden.

Wir empfehlen, die TTL in den folgenden NS-Datensätzen zu ändern:

- Im NS-Datensatz in der gehosteten Zone für den aktuellen DNS-Dienstanbieter. (Ihr aktueller Anbieter verwendet möglicherweise eine andere Terminologie.)
- Im NS-Datensatz in der gehostete Zone, die Sie in Schritt 2: Erstellen einer gehosteten Zone erstellt haben.

So senken Sie die TTL-Einstellung im NS-Datensatz für den aktuellen DNS-Dienstanbieter

- Verwenden Sie die Methode, die vom aktuellen DNS-Serviceanbieter für die Domäne zur Verfügung gestellt wird, um die TTL für den NS-Datensatz in der gehosteten Zone für Ihre Domäne zu ändern.

So senken Sie die TTL-Einstellung im NS-Datensatz in einer gehosteten Route 53-Zone

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den Namen der gehosteten Zone aus.
4. Wählen Sie den NS-Datensatz und anschließend ausBearbeitenaus.
5. Ändern Sie den Wert TTL (Seconds). Wir empfehlen, einen Wert zwischen 60 Sekunden und 900 Sekunden (15 Minuten) anzugeben.
6. Wählen Sie Save Changes (Änderungen speichern).

Schritt 5: (Wenn Sie DNSSEC konfiguriert haben) Entfernen Sie den DS-Eintrag aus der übergeordneten Zone

Wenn Sie DNSSEC für Ihre Domäne konfiguriert haben, entfernen Sie den Eintrag Delegation Signer (DS) aus der übergeordneten Zone, bevor Sie Ihre Domäne zu Route 53 migrieren.

Wenn die übergeordnete Zone über Route 53 oder eine andere Vergabestelle gehostet wird, kontaktieren Sie sie, um den DS-Datensatz zu entfernen.

Da es derzeit nicht möglich ist, die DNSSEC-Signatur bei zwei Anbietern zu aktivieren, müssen Sie alle DS entfernen oder DNSKEYs DNSSEC deaktivieren. Dies signalisiert DNS-Resolvern vorübergehend, die DNSSEC-Validierung zu deaktivieren. In Schritt 11können Sie die DNSSEC-Validierung bei Bedarf wieder aktivieren, nachdem der Übergang zu Route 53 abgeschlossen ist.

Weitere Informationen finden Sie unter Löschen von öffentlichen Schlüsseln für eine Domäne.

Schritt 6: Warten, bis die alte TTL abgelaufen ist

Wenn Ihre Domäne verwendet wird (z. B. wenn Ihre Benutzer den Domänennamen verwenden, um eine Website zu suchen oder auf eine Webanwendung zuzugreifen), dann wurden die Namen der Namenserver, die von Ihrem aktuellen DNS-Serviceanbieter zur Verfügung gestellt wurden, von DNS-Resolvern zwischengespeichert. Ein DNS-Resolver, der diese Informationen einige Minuten zuvor zwischengespeichert hat, hält sie fast zwei weitere Tage gespeichert.

Um sicherzustellen, dass die Migration des DNS-Service zu Route 53 zum gleichen Zeitpunkt erfolgt, warten Sie zwei Tage, nachdem Sie die TTL gesenkt haben. Nachdem die zweitägige TTL abgelaufen ist und die Resolver den Namenserver für Ihre Domäne anfordern, rufen die Resolver die aktuellen Namenserver sowie die neue TTL ab, die Sie in Schritt 4: Senken der TTL-Einstellungen angegeben haben.

Schritt 7: Aktualisieren Sie die NS-Einträge, um Route 53-Nameserver zu verwenden

Um Amazon Route 53 als DNS-Dienst für eine Domäne zu verwenden, nutzen Sie die vom aktuellen DNS-Dienstanbieter bereitgestellte Methode, um die aktuellen Namenserver im NS-Datensatz durch Route 53-Namenserver zu ersetzen.

> **Note**
>
> Wenn Sie den NS-Eintrag mit dem aktuellen DNS-Dienstanbieter aktualisieren, um Route 53 -Namensserver zu verwenden, aktualisieren Sie die DNS-Konfiguration für die Domäne. (Dies ist vergleichbar mit dem Aktualisieren des NS-Datensatzes in der gehosteten Route 53-Zone für eine Domäne, mit der Ausnahme, dass Sie die Einstellung mit dem DNS-Service aktualisieren, von dem Sie weggehen.)

So aktualisieren Sie den NS-Eintrag im Registrar oder in der übergeordneten Zone, um Route 53-Namenserver zu verwenden

1. Rufen Sie in der Route 53-Konsole die Namenserver für Ihre gehostete Zone ab:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/

   b. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

   c. Wählen Sie auf der Seite Hosted zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gültige gehostete Zone aus.

   d. Notieren Sie sich die vier Namen, die für Namensserver im Abschnitt Hosted zone details (Details der gehosteten Zone) erstellt.

2. Verwenden Sie die Methode, die vom aktuellen DNS-Dienst für die Domäne zur Verfügung gestellt wird, um die NS-Datensätze für die gehostete Zone zu aktualisieren. Wenn die Domäne bei Route 53 registriert wurde, lesen Sie Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.Der Prozess hängt davon ab, ob Sie mit dem aktuellen DNS-Dienst Nameserver löschen können:

   Wenn Sie Namenserver löschen können

   - Notieren Sie die Namen der aktuellen Nameserver im NS-Datensatz für die gehostete Zone. Geben Sie diese Server an, wenn Sie das System auf die aktuelle DNS-Konfiguration zurücksetzen müssen.
   - Löschen Sie die aktuellen Nameserver aus dem NS-Datensatz.
   - Aktualisieren Sie den NS-Datensatz mit den Namen aller vier Route 53-Nameserver, die Sie in Schritt 1 dieses Verfahrens erhalten haben.

   > **Note**
   >
   > Anschließend sind nur noch die vier Route 53 -Nameserver im NS-Datensatz enthalten.

   Wenn Sie Namenserver nicht löschen können

   - Wählen Sie die Option zum Verwenden benutzerdefinierter Nameserver aus.
   - Fügen Sie alle vier Route 53-Nameserver hinzu, die Sie in Schritt 1 erhalten haben.

Schritt 8: Überwachen des Datenverkehrs für die Domäne

Überwachen Sie den Datenverkehr für die Domäne, einschließlich des Datenverkehrs für die Website oder Anwendung, und E-Mail:

- Wenn der Datenverkehr langsamer wird oder abbricht - Verwenden Sie die Methode des vorherigen DNS-Dienst, um die Namenserver für die Domäne wieder in die vorherigen Namenserver zu ändern. Hierbei handelt es sich um die Namenserver, die Sie unter in Schritt 7 von So aktualisieren Sie den NS-Eintrag im Registrar oder in der übergeordneten Zone, um Route 53-Namenserver zu verwenden notiert haben. Ergründen Sie anschließend, was schiefgelaufen ist.
- Wenn der Datenverkehr nicht betroffen ist - Fahren Sie mit Schritt 9: Zurückändern der TTL für den NS-Datensatz in einen höheren Wert fort.

Schritt 9: Zurückändern der TTL für den NS-Datensatz in einen höheren Wert

Ändern Sie die TTL für den NS-Datensatz in der gehosteten Amazon Route 53-Zone für die Domäne in einen typischen Wert, z. B. 172800 Sekunden (2 Tage). Dadurch wird die Latenz für Ihre Benutzer verbessert, da sie nicht so oft darauf warten müssen, dass DNS-Resolver eine Abfrage für die Namenserver Ihrer Domäne senden.

So ändern Sie die TTL für den NS-Datensatz in der gehosteten Route 53-Zone

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den Namen der gehosteten Zone aus.
4. Wählen Sie in der Liste der Datensätze für die gehostete Zone den NS-Datensatz aus.
5. Wählen Sie Edit (Bearbeiten) aus.
6. Ändern Sie den Wert TTL (Seconds) in die Anzahl von Sekunden, die DNS-Resolver die Namen der Namenserver für Ihre Domäne zwischenspeichern sollen. Wir empfehlen einen Wert von 172 800 Sekunden.
7. Wählen Sie Save Changes (Änderungen speichern).

Schritt 10: Übertragen der Domänenregistrierung an Amazon Route 53

Nachdem Sie den DNS-Dienst für eine Domäne an Amazon Route 53 übertragen haben, können Sie die Registrierung für die Domäne optional an Route 53 übertragen. Weitere Informationen finden Sie unter Übertragen der Registrierung für eine Domain an Amazon Route 53.

Schritt 11: DNSSEC-Signatur erneut aktivieren (falls erforderlich)

Nachdem Sie den DNS-Dienst für eine Domäne an Amazon Route 53 übertragen haben, können Sie die DNSSEC-Signatur erneut aktivieren.

Das Aktivieren der DNSSEC-Signatur erfolgt in zwei Schritten:

- Schritt 1: Aktivieren Sie die DNSSEC-Signatur für Route 53 und fordern Sie Route 53 auf, einen Key Signing Key (KSK) auf der Grundlage eines vom Kunden verwalteten Schlüssels in AWS Key Management Service () zu erstellen.AWS KMS
- Schritt 2: Erstellen Sie eine Vertrauenskette für die gehostete Zone, indem Sie einen Delegation Signer (DS)-Datensatz zur übergeordneten Zone hinzufügen, damit DNS-Antworten mit vertrauenswürdigen kryptografischen Signaturen authentifiziert werden können.

  Detaillierte Anweisungen finden Sie unter Aktivieren der DNSSEC-Signierung und Aufbau einer Vertrauenskette.

Route 53 als DNS-Dienst für eine inaktive Domäne nutzen

Wenn Sie den DNS-Dienst zu Amazon Route 53 für eine Domäne migrieren möchten, die keinen (oder nur sehr wenig Datenverkehr) erhält, führen Sie die Schritte in diesem Abschnitt aus.

Themen

Schritt 1: Abrufen Ihrer aktuellen DNS-Konfiguration vom aktuellen DNS-Dienstanbieter (inaktive Domänen)

Wenn Sie einen DNS-Service von einem anderen Anbieter zu Route 53 migrieren, reproduzieren Sie Ihre aktuelle DNS-Konfiguration in Route 53. Erstellen Sie in Route 53 erst eine gehostete Zone mit demselben Namen wie Ihre Domäne und dann Datensätze in dieser gehosteten Zone. Jeder Datensatz gibt an, wie der Datenverkehr für einen bestimmten Domänen- oder Subdomänennamen weitergeleitet werden soll. Wenn beispielsweise jemand Ihren Domainnamen in einen Webbrowser eingibt, möchten Sie, dass der Datenverkehr an einen Webserver in Ihrem Rechenzentrum, an eine EC2 Amazon-Instance, an eine CloudFront Distribution oder an einen anderen Ort weitergeleitet wird?

Der Prozess, den Sie verwenden, hängt von der Komplexität Ihrer aktuellen DNS-Konfiguration ab:

- Wenn Ihre aktuelle DNS-Konfiguration einfach ist - Wenn Sie den Internetdatenverkehr nur für einige Subdomänen an eine geringe Anzahl von Ressourcen, wie Webserver oder Amazon-S3-Buckets, weiterleiten, können Sie einige Datensätze in der Route 53-Konsole manuell erstellen.
- Wenn Ihre aktuelle DNS-Konfiguration eher komplex ist und Sie Ihre aktuelle Konfiguration lediglich reproduzieren möchten - Sie können die Migration vereinfachen, wenn Sie eine Zonendatei vom aktuellen DNS-Dienstanbieter abrufen können, und die Zonendatei in Route 53 importieren. (Nicht alle DNS-Dienstanbieter stellen Zonendateien zur Verfügung.) Beim Importieren einer Zonendatei reproduziert Route 53 die vorhandene Konfiguration automatisch, indem die entsprechenden Datensätze in Ihrer gehosteten Zone erstellt werden.

  Fragen Sie beim Kundenservice Ihres aktuellen DNS-Dienstanbieters nach, wie Sie eine Zonendatei oder eine Datensatzliste erhalten. Informationen über das erforderliche Format der Zonendatei finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.
- Wenn Ihre aktuelle DNS-Konfiguration eher komplex ist und Sie an Route 53-Routing-Funktionen interessiert sind - Sehen Sie sich die folgende Dokumentation an, um festzustellen, ob Sie Route 53-Funktionen verwenden möchten, die von anderen DNS-Dienstanbietern nicht zur Verfügung gestellt werden. Wenn dies der Fall ist, können Sie entweder Datensätze manuell erstellen oder eine Zonendatei importieren und Datensätze zu einem späteren Zeitpunkt erstellen oder aktualisieren:
  - Wählen zwischen Alias- und Nicht-Alias-Datensätzenerklärt die Vorteile von Route 53-Aliasdatensätzen, die den Datenverkehr kostenlos an einige AWS Ressourcen wie CloudFront Distributionen und Amazon S3 S3-Buckets weiterleiten.

- Auswählen einer Routing-Richtlinie erläutert die Route 53-Routing-Optionen, z. B. Routing basierend auf dem Standort Ihrer Benutzer, Routing auf Basis der Latenz zwischen Ihren Benutzern und Ressourcen, Routing basierend darauf, ob Ihre Ressourcen fehlerfrei sind, und Routing an Ressourcen basierend auf den von Ihnen angegebenen Gewichtungen.

> **Note**
>
> Sie können eine Zonendatei auch importieren und die Konfiguration zu einem späteren Zeitpunkt ändern, um Aliasdatensätze und komplexe Routing-Richtlinien zu nutzen.

Wenn Sie keine Zonendatei abrufen können oder Datensätze in Route 53 manuell erstellen möchten, müssen Sie wahrscheinlich u. a. folgende Datensätze migrieren:

- A (Address) -Datensätze — verknüpfen einen Domainnamen oder Subdomänennamen mit der IPv4 Adresse (z. B. 192.0.2.3) der entsprechenden Ressource
- AAAA-Einträge (Address) — verknüpfen einen Domainnamen oder Subdomainnamen mit der IPv6 Adresse (z. B. 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) der entsprechenden Ressource
- MX-Datensätze (Mail Server) - Datenverkehr an Mail-Server weiterleiten
- CNAME-Datensätze - Den Datenverkehr für einen Domänennamen (example.net) an einen anderen Domänennamen (example.com) weiterleiten
- Datensätze für andere unterstützte DNS-Datensatztypen - Eine Liste der unterstützen Datensatztypen finden Sie unter Unterstützte DNS-Datensatztypen.

Schritt 2: Erstellen einer gehosteten Zone (inaktive Domänen)

Um Amazon Route 53 mitzuteilen, wie Sie den Datenverkehr für Ihre Domäne weiterleiten möchten, erstellen Sie zuerst eine gehostete Zone mit demselben Namen wie Ihre Domäne und dann die Datensätze in der gehosteten Zone.

> **Important**
>
> Sie können eine gehostete Zone nur für eine Domäne erstellen, die Sie über die Berechtigung zur Verwaltung verfügen. Das heißt in der Regel, dass Sie Eigentümer der Domäne sind. Es könnte aber auch bedeuten, dass Sie eine Anwendung für den Eigentümer entwickeln.

Bei der Erstellung einer gehosteten Zone erstellt Route 53 automatisch einen NS-Eintrag (Namenserver) und einen SOA-Eintrag (Start of Authority, Autoritätsursprung) für die Zone. Der NS-Datensatz identifiziert die vier Namenserver, die Route 53 Ihrer gehosteten Zone zugeordnet hat. Um Route 53 als DNS-Dienst für Ihre Domäne festzulegen, aktualisieren Sie die Registrierung für die Domäne mit diesen vier Namenservern.

> **Important**
>
> Erstellen Sie keine zusätzlichen NS- (Namenserver) oder SOA-Datensätze (Autoritätsursprung) und löschen Sie die vorhandenen NS- und SOA-Datensätze nicht.

So erstellen Sie eine gehostete Zone

1. Melden Sie sich bei https://console.aws.amazon.com/route53/der an und öffnen AWS-Managementkonsole Sie die Route 53-Konsole unter.
2. Wenn Sie noch keine Erfahrung mit Route 53 haben, wählen Sie Get Started (Erste Schritte) aus.

   Wenn Sie Route 53 bereits nutzen, wählen Sie Hosted zones im Navigationsbereich aus.
3. Wählen Sie Create Hosted Zone (Gehostete Zone erstellen).
4. Geben Sie im Bereich Create Hosted Zone (Gehostete Zone erstellen) einen Domänennamen und optional einen Kommentar ein. Weitere Informationen über Einstellungen erhalten Sie in Quickinfos, wenn Sie mit dem Mauszeiger auf die jeweilige Beschriftung zeigen.

   Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.
5. Übernehmen Sie für Type den Standardwert Public Hosted Zone.
6. Wählen Sie Create hosted zone (Gehostete Zone erstellen) aus.

Schritt 3: Erstellen von Datensätzen (inaktive Domänen)

Nachdem Sie eine gehostete Zone angelegt haben, erstellen Sie Datensätze in der gehosteten Zone, die definieren, wie Sie den Datenverkehr für eine Domäne (example.com) oder Subdomäne (www.example.com) weiterleiten möchten. Wenn Sie beispielsweise Traffic für example.com und www.example.com an einen Webserver auf einer EC2 Amazon-Instance weiterleiten möchten,

erstellen Sie zwei Datensätze, einen mit dem Namen example.com und den anderen mit dem Namen www.example.com. In jedem Datensatz geben Sie die IP-Adresse für Ihre Instance an. EC2

Für das Erstellen von Datensätzen gibt es verschiedene Möglichkeiten:

Importieren einer Zonendatei

Dies ist die einfachste Methode, wenn Sie eine Zonendatei von Ihrem aktuellen DNS-Dienst in erhalten haben Schritt 1: Abrufen Ihrer aktuellen DNS-Konfiguration vom aktuellen DNS-Dienstanbieter (inaktive Domänen). Amazon Route 53 kann nicht vorhersagen, wann Aliasdatensätze erstellt oder spezielle Routing-Typen wie gewichtete oder Failover-Datensätze verwendet werden sollen. Daher erstellt Route 53 DNS-Standarddatensätze mithilfe der einfachen Routing-Richtlinie, wenn Sie eine Zonendatei importieren.

Weitere Informationen finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.

Erstellen von einzelnen DNS-Datensätzen in der Konsole

Wenn Sie keine Zonendatei erhalten haben und nur einige Datensätze mit der einfachen Routing-Richtlinie für die ersten Schritte erstellen möchten, können Sie die Datensätze in der Route 53 - Konsole erstellen. Sie können sowohl Alias- als auch Nicht-Alias-Datensätze erstellen.

Weitere Informationen finden Sie unter den folgenden Themen:

- Auswählen einer Routing-Richtlinie
- Wählen zwischen Alias- und Nicht-Alias-Datensätzen
- Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole

Programmgesteuertes Erstellen von Datensätzen

Sie können Datensätze erstellen, indem Sie einen der Befehle AWS SDKs AWS CLI, den oder verwenden AWS Tools for Windows PowerShell. Weitere Informationen finden Sie in der AWS Dokumentation.

Wenn Sie eine Programmiersprache verwenden, für die AWS kein SDK bereitgestellt wird, können Sie auch die Route 53-API verwenden. Weitere Informationen finden Sie unter Amazon Route 53 API Reference.

Schritt 4: Aktualisieren der Domänenregistrierung zur Verwendung von Amazon-Route-53-Nameservern (inaktive Domänen)

Nachdem Sie die Datensätze für die Domäne erstellt haben, können Sie den DNS-Service für Ihre Domäne in Amazon Route 53 ändern. Führen Sie die folgenden Schritte aus, um die Einstellungen bei der Domänenvergabestelle zu aktualisieren.

So aktualisieren Sie die Namenserver für die Domäne

1. Rufen Sie die Nameserver für eine öffentliche gehostete Zone mithilfe der Route 53-Konsole ab.
   a. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
   b. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
   c. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone aus, und dann View details (Details anzeigen).
   d. Wählen Sie auf der Detailseite für die gehostete Zone Hosted Zone details (Details der gehosteten Zone) aus.
   e. Notieren Sie sich die vier Namen, die für Name Servers (Namenserver) aufgelistet werden.
2. Ändern Sie unter Verwendung der von der Vergabestelle für die Domäne bereitgestellten Methode die Namenserver für die Domäne in die vier Route 53-Namenserver, die Sie in Schritt 2 dieses Verfahrens erhalten haben.

   Wenn die Domäne mit Route 53 registriert wurde, lesen Sie Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Konfigurieren von DNS-Routing für eine neue Domäne

Eine neue Domain, die Sie bei Route 53 gekauft haben

Wenn Sie eine Domäne bei Route 53 registrieren, machen wir Route 53 automatisch als DNS-Service für die Domäne. Route 53 erstellt eine gehostete Zone, die denselben Namen wie die Domäne hat, weist der gehosteten Zone vier Namenserver zu und aktualisiert die Domäne zur Verwendung dieser Nameserver.

Eine neue Domain, die Sie bei einem anderen Registrar gekauft haben

Wenn Sie beispielsweise eine Domain von einem anderen Registrar kaufen, weil die Top-Level-Domain (TLD) nicht von Route 53 angeboten wird, haben Sie zwei Möglichkeiten:

- Verwenden Sie Route 53 nur für DNS-Hosting: Behalten Sie Ihren aktuellen Registrar, aber delegieren Sie die DNS-Verwaltung an Route 53. Gehen Sie wie folgt vor, um eine gehostete Zone zu erstellen und die Nameserver Ihres Registrars zu aktualisieren.
- Übertragen Sie die Domainregistrierung auf Route 53: Machen Sie Route 53 zu Ihrem Registrar und DNS-Dienst. Informationen zu Checkliste vor der Übertragung für Domainübertragungen den Voraussetzungen und Übertragen der Registrierung für eine Domain an Amazon Route 53 zum Übertragungsprozess finden Sie unter.

Weitere Informationen zur TLDs Unterstützung durch Route 53 finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können.

Folgen Sie diesen Anweisungen, um eine öffentlich gehostete Zone zu erstellen und dann die mit dem Registrar erstellten Nameserver zu verwenden:

So erstellen Sie eine gehostete Zone für eine Domäne, die nicht zu Route 53 gehört

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Gehostete Zonen aus und wählen Sie dann Gehostete Zone erstellen aus.
3. Geben Sie als Name den Namen der Domain ein, für die Sie eine Hosting-Zone erstellen möchten, z. B. eine optionale Beschreibung`example.com`, wählen Sie Public Hosted Zone und dann Create Hosted Zone aus.
4. Nachdem Sie die Hosting-Zone erstellt haben, notieren Sie sich die vier Nameserver-Einträge (NS), die erstellt wurden. Jeder beginnt mit „ns-“.

   Geben Sie bei Ihrem Domain-Registrar die Nameserver von oben ein, um die Domainverwaltung an Ihre von Route 53 gehostete Zone zu delegieren.

DNS-Verkehr weiterleiten

Um anzugeben, wie Route 53 den Datenverkehr für die Domäne weiterleiten soll, erstellen Sie Datensätze in der gehosteten Zone. Wenn Sie beispielsweise Anfragen für example.com an einen Webserver weiterleiten möchten, der auf einer EC2 Amazon-Instance läuft, erstellen Sie einen Datensatz in der gehosteten Zone example.com und geben die Elastic IP-Adresse für die EC2 Instance an. Weitere Informationen finden Sie unter den folgenden Themen:

- Weitere Informationen zum Erstellen von Datensätzen in Ihrer gehosteten Zone finden Sie unter Arbeiten mit Datensätzen.
- Informationen darüber, wie Sie Traffic zu ausgewählten AWS Ressourcen weiterleiten, finden Sie unter. Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen
- Weitere Information zur Funktionsweise von DNS finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird.
- Informationen zur Überprüfung der DNS-Speicherung finden Sie unterÜberprüfen der DNS-Antworten von Route 53.

Weiterleiten des Datenverkehrs an Ihre Ressourcen

Wenn Benutzer Ihre Website oder Webanwendung anfordern, indem sie beispielsweise den Namen Ihrer Domäne in einen Webbrowser eingeben, hilft Route 53 dabei, Benutzer zu Ihren Ressourcen wie einem Amazon-S3-Bucket oder einem Webserver in Ihrem Rechenzentrum zu leiten. Zum Konfigurieren von Route 53 zur Weiterleitung des Datenverkehrs an Ihre Ressourcen gehen Sie wie folgt vor:

1. Erstellen Sie eine gehostete Zone. Sie können eine öffentliche gehostete Zone oder eine private gehostete Zone erstellen:

   Öffentliche gehostete Zone

   Erstellen Sie eine öffentlich gehostete Zone, wenn Sie beispielsweise Internetverkehr zu Ihren Ressourcen weiterleiten möchten, damit Ihre Kunden die Unternehmenswebsite aufrufen können, die Sie auf EC2 Instances hosten. Weitere Informationen finden Sie unter Arbeiten mit öffentlichen gehosteten Zonen.

   Privat gehostete Zone

   Erstellen Sie eine private gehostete Zone, wenn Sie den Datenverkehr innerhalb einer Amazon VPC weiterleiten wollen. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.
2. Erstellen von Datensätzen in der gehosteten Zone. Datensätze definieren, wohin der Datenverkehr für einen bestimmten Domänen- oder Subdomänennamen weitergeleitet werden soll. Um beispielsweise den Datenverkehr für www.example.com zu einem Webserver in Ihrem Rechenzentrum weiterzuleiten, erstellen Sie in der Regel einen www.example.com-Datensatz in der gehosteten Zone example.com.

Weitere Informationen finden Sie unter den folgenden Themen:

- Arbeiten mit Datensätzen
- Weiterleiten von Datenverkehr für Subdomänen
- Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen

Weiterleiten von Datenverkehr für Subdomänen

Wenn Sie Datenverkehr zu Ihren Ressourcen für eine Subdomäne wie acme.example.com oder zenith.example.com weiterleiten möchten, haben Sie zwei Möglichkeiten:

Sie erstellen Datensätze in der gehosteten Zone für die Domäne

Um den Datenverkehr für eine Subdomäne weiterzuleiten, erstellen Sie normalerweise einen Datensatz in der gehosteten Zone, der den gleichen Namen wie die Domäne hat. Um beispielsweise den Internet-Datenverkehr für acme.example.com zu einem Webserver in Ihrem Rechenzentrum weiterzuleiten, erstellen Sie in der Regel einen Datensatz namens acme.example.com in der gehosteten Zone example.com. Weitere Informationen finden Sie unter dem Thema Arbeiten mit Datensätzen und seinen Unterthemen.

Sie erstellen eine gehostete Zone für die Subdomäne und erstellen Datensätze in der neuen gehosteten Zone

Sie können auch eine gehostete Zone für die Subdomäne erstellen. Die Verwendung einer separaten gehosteten Zone zum Weiterleiten von Internetverkehr für eine Subdomäne wird manchmal als „Delegieren der Verantwortung für eine Subdomäne an eine gehostete Zone“ oder als „Delegieren einer Subdomäne an andere Nameserver“ oder als eine ähnliche Kombination von Begriffen bezeichnet. Im Folgenden finden Sie eine Übersicht über die Funktionsweise:

1. Sie erstellen eine gehostete Zone, die denselben Namen wie die Subdomäne hat, für die Sie Datenverkehr weiterleiten möchten, z. B. acme.example.com.
2. Anschließend erstellen Sie Datensätze in der neuen gehosteten Zone, die definieren, wie Sie den Datenverkehr für die Subdomäne (acme.example.com) und deren Unterdomänen weiterleiten möchten, wie z. B. backend.acme.example.com.
3. Sie erhalten die Nameserver, die Route 53 der neuen gehosteten Zone zugewiesen hat, als sie von ihnen erstellt wurde.

4. Sie erstellen einen neuen NS-Eintrag in der Hosting-Zone für die Domain (example.com). Der Name des NS-Eintrags muss der Subdomänenname (acme.example.com) sein, und Sie geben die vier Nameserver, die Sie in Schritt 3 erhalten haben, als Datensatzwerte an.

Wenn Sie eine separate gehostete Zone zum Weiterleiten des Datenverkehrs für eine Subdomäne verwenden, können Sie mithilfe von IAM-Berechtigungen den Zugriff auf die gehostete Zone für die Subdomäne beschränken. Wenn Sie mehrere Subdomänen haben, die von verschiedenen Gruppen verwaltet werden, kann das Erstellen einer gehosteten Zone für jede Subdomäne die Anzahl der Personen, die Zugriff auf Datensätze in der gehosteten Zone für die Domäne haben müssen, erheblich reduzieren.

Um diesen Delegierungsprozess zu implementieren, benötigen Sie die folgenden IAM-Berechtigungen. Weitere Informationen zu Route 53 53-IAM-Richtlinien finden Sie unterIdentity and Access Management in Amazon Route 53:

Elternkonto (besitzt example.com)

Der Benutzer oder die Rolle benötigt Berechtigungen, um Datensätze in der Hosting-Zone der übergeordneten Domain zu ändern:

Kinderkonto (erstellt acme.example.com)

Der Benutzer oder die Rolle benötigt Berechtigungen, um die gehostete Subdomain-Zone zu erstellen und zu verwalten:

Wenn Sie eine separate gehostete Zone für eine Subdomäne verwenden, können Sie auch andere DNS-Dienste für die Domäne und die Subdomäne verwenden. Weitere Informationen finden Sie unter Verwendung von Amazon Route 53 als DNS-Service für eine Subdomäne ohne Migration der übergeordneten Domäne.

Es entsteht eine geringe Auswirkung auf die Performance dieser Konfiguration bei der ersten DNS-Abfrage von jedem DNS-Auflöser. Der Auflöser muss Informationen von der gehosteten Zone für die Stammdomäne und dann von der gehosteten Zone für die Subdomäne erhalten. Nach der ersten DNS-Abfrage für eine Subdomäne speichert der Auflöser die Informationen und muss sie nicht erneut abrufen, bis die TTL abläuft und ein anderer Client die Subdomäne von diesem Auflöser anfordert. Weitere Informationen finden Sie unter TTL (Sekunden) im Abschnitt Werte, die Sie beim Erstellen oder Bearbeiten von Amazon Route 53-Datensätzen angeben.

Themen

- Erstellen einer anderen gehosteten Zone zur Weiterleitung des Datenverkehrs für eine Subdomäne

- Weiterleiten von Datenverkehr für zusätzliche Ebenen von Subdomänen

Erstellen einer anderen gehosteten Zone zur Weiterleitung des Datenverkehrs für eine Subdomäne

Eine Möglichkeit, den Datenverkehr für eine Subdomäne weiterzuleiten, besteht darin, eine gehostete Zone für die Subdomäne zu erstellen und dann Datensätze für die Subdomäne in der neuen gehosteten Zone zu erstellen. (Die gebräuchlichere Option ist, Datensätze für die Subdomäne in der gehosteten Zone für die Domäne zu erstellen.)

> **Note**
>
> Dieses Verfahren zeigt, wie eine Subdomain an Route 53 delegiert wird. Sie können eine Subdomain auch an andere DNS-Dienste delegieren, indem Sie stattdessen NS-Einträge erstellen, die auf die Nameserver dieser Dienste verweisen.

Es folgt eine Übersicht über den Prozess:

1. Erstellen einer gehosteten Zone für die Subdomäne. Weitere Informationen finden Sie unter Erstellen einer neuen gehosteten Zone für eine Subdomäne.
2. Hinzufügen von Datensätzen für die Subdomäne zu der gehosteten Zone. Wenn die gehostete Zone für die Domäne Datensätze enthält, die in die gehostete Zone für die Subdomäne gehören, duplizieren Sie diese Datensätze in der gehosteten Zone für die Subdomäne. Weitere Informationen finden Sie unter Erstellen von Datensätzen in der gehosteten Zone für die Subdomäne
3. Erstellen Sie einen NS-Datensatzes für die Subdomäne in der gehosteten Zone für die Domäne, wodurch die Verantwortung für die Subdomäne an die Namensserver in der neuen gehosteten Zone delegiert wird. Wenn die gehostete Zone für die Domäne Datensätze enthält, die in die gehostete Zone für die Subdomäne gehören, löschen Sie die Datensätze aus der gehosteten Zone für die Domäne. (Sie haben Kopien in der gehosteten Zone für die Subdomäne in Schritt 2 erstellt.) Weitere Informationen finden Sie unter Aktualisieren der gehosteten Zone für die Domäne.

Erstellen einer neuen gehosteten Zone für eine Subdomäne

Zum Erstellen einer gehosteten Zone für eine Subdomäne unter Verwendung der Route 53-Konsole führen Sie die folgenden Schritte aus.

Erstellen einer gehosteten Zone für eine Subdomäne (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wenn Sie noch keine Erfahrung mit Route 53 haben, wählen Sie Get Started (Erste Schritte) aus.

   Wenn Sie Route 53 bereits nutzen, wählen Sie Hosted zones im Navigationsbereich aus.
3. Wählen Sie Create Hosted Zone.
4. Geben Sie im Bereich rechts den Namen der Unterdomäne ein, zum Beispiel acme.example.com. Optional können Sie auch einen Kommentar eingeben.

   Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.
5. Übernehmen Sie für Type den Standardwert Public Hosted Zone.
6. Wählen Sie im rechten Bereich unten die Option Create (Erstellen) aus.

Erstellen von Datensätzen in der gehosteten Zone für die Subdomäne

Um festzulegen, wie Route 53 den Datenverkehr für die Subdomäne (acme.example.com) und ihre Subdomänen (backend.acme.example.com) weiterleiten soll, erstellen Sie Datensätze in der gehosteten Zone für die Subdomäne.

Beachten Sie Folgendes zum Erstellen von Datensätzen in der gehosteten Zone für die Subdomäne:

- Erstellen Sie keine zusätzlichen Namensserver (NS)- oder Autoritätsursprung (SOA)-Datensätze in der gehosteten Zone für die Subdomäne, und löschen Sie nicht die vorhandenen NS- und SOA-Datensätze.
- Erstellen Sie alle Datensätze für die Subdomäne in der gehosteten Zone für die Subdomäne. Wenn Sie beispielsweise Zonen für example.com und für die Domäne acme.example.com gehostet haben, erstellen Sie alle Datensätze für die Unterdomäne acme.example.com in der gehosteten Zone acme.example.com. Dazu gehören Datensätze wie backend.acme.example.com und beta.backend.acme.example.com.
- Wenn die gehostete Zone für die Domäne (example.com) bereits Datensätze enthält, die in die gehostete Zone für die Subdomäne (acme.example.com) gehören, kopieren Sie diese Datensätze

in der gehosteten Zone für die Subdomäne. Im letzten Schritt des Prozesses löschen Sie die doppelten Datensätze aus der gehosteten Zone für die Domäne später.

> **Important**
>
> Wenn Sie sowohl in der gehosteten Zone für die Domäne als auch in der gehosteten Zone für die Subdomäne Datensätze für die Subdomäne haben, ist das DNS-Verhalten inkonsistent. Das Verhalten hängt davon ab, welche Nameserver ein DNS-Resolver zwischengespeichert hat, die Nameserver für die gehostete Zone der Domäne (example.com) oder die Nameserver für die gehostete Zone der Subdomäne (acme.example.com). In einigen Fällen gibt Route 53 NXDomäne (nicht vorhandene Domäne) zurück, wenn der Datensatz vorhanden ist, jedoch nicht in der gehosteten Zone, an die DNS-Resolver die Abfrage senden.

Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

Aktualisieren der gehosteten Zone für die Domäne

Wenn Sie eine gehostete Zone erstellen, weist Route 53 der Zone automatisch vier Namensserver zu. Der NS-Eintrag für eine gehostete Zone identifiziert die Nameserver, die auf DNS-Abfragen für die Domäne oder Subdomäne reagieren. Um die Datensätze in der gehosteten Zone für die Subdomäne zur Weiterleitung des Internetverkehrs zu verwenden, erstellen Sie einen neuen NS-Datensatz in der gehosteten Zone für die Domäne (example.com) und geben ihm den Namen der Subdomäne (acme.example.com). Für den Wert des NS-Datensatzes geben Sie die Namen der Nameserver aus der gehosteten Zone für die Subdomäne an.

Das passiert, wenn Route 53 eine DNS-Abfrage von einem DNS-Auflöser für die Subdomäne acme.example.com oder eine ihrer Subdomänen erhält:

1. Route 53 sucht in der gehosteten Zone nach der Domäne (example.com) und findet den NS-Datensatz für die Subdomäne (acme.example.com).
2. Route 53 ruft die Nameserver vom NS-Eintrag acme.example.com in der gehosteten Zone für die Domäne example.com ab und gibt diese Nameserver an den DNS-Resolver zurück.
3. Der Auflöser sendet die Anfrage für acme.example.com erneut an die Namensserver der gehosteten Zone acme.example.com.
4. Route 53 beantwortet die Abfrage unter Verwendung eines Datensatzes in der gehosteten Zone acme.example.com.

Führen Sie die folgenden Schritte aus, um Route 53 so zu konfigurieren, dass der Datenverkehr für die Subdomäne mithilfe der gehosteten Zone für die Subdomäne weitergeleitet und doppelte Datensätze aus der gehosteten Zone für die Domäne gelöscht werden:

So konfigurieren Sie Route 53 für die Verwendung der gehosteten Zone für die Subdomäne (Konsole)

1. Rufen Sie in der Route 53-Konsole die Namensserver für die gehostete Zone für die Subdomäne ab:
   a. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
   b. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone für die Subdomäne aus.
   c. Kopieren Sie im rechten Bereich die Namen der vier Server, die für Name Server im Bereich Details zur gehosteten Zone aufgeführt sind.
2. Wählen Sie den Namen der gehosteten Zone für die Domäne (example.com), nicht für die Subdomäne.
3. Wählen Sie Datensatz erstellen.
4. Wählen Sie Simple Routing (Einfaches Routing), und wählen Sie Next (Weiter).
5. Wählen Sie Define simple record (Einfachen Datensatz definieren).
6. Geben Sie die folgenden Werte an:

   Name

   Geben Sie den Namen der Subdomain ein (z. B.`acme.example.com`). Dieser muss genau mit dem Namen der von Ihnen erstellten Subdomain-Hosting-Zone übereinstimmen.

   Bewerten/Weiterleiten des Datenverkehrs an

   Klicken Sie aufIP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp, und fügen Sie die Namen der Namenserver ein, die Sie in Schritt 1 kopiert haben.

   Datensatztyp

   Klicken Sie aufNS — Namenserver für eine gehostete -Zone:aus.

   TTL (Sekunden)

   Ändern Sie dies in einen gebräuchlicheren Wert für einen NS-Datensatz, z. B. 172800 Sekunden.

7. Klicken Sie aufEinfachen Datensatz definieren, und wählen SieErstellen von Datensätzenaus.
8. Wenn die gehostete Zone für die Domäne Datensätze enthält, die Sie in der gehosteten Zone für die Subdomäne neu erstellt haben, löschen Sie diese Datensätze aus der gehosteten Zone für die Domäne. Weitere Informationen finden Sie unter Löschen von Datensätzen.

   Wenn Sie fertig sind, sollten sich alle Datensätze für die Subdomäne in der gehosteten Zone für die Subdomäne befinden.

Weiterleiten von Datenverkehr für zusätzliche Ebenen von Subdomänen

Sie leiten Datenverkehr zu einer Subdomäne einer Subdomäne, wie z. B. backend.acme.example.com, genauso weiter, wie Sie Datenverkehr zu einer Subdomäne weiterleiten, wie z. B. acme.example.com. Entweder Sie erstellen Datensätze in der gehosteten Zone für die Domäne, oder Sie erstellen eine gehostete Zone für die untergeordnete Subdomäne, und dann erstellen Sie Datensätze in dieser neuen gehosteten Zone.

Wenn Sie eine separate gehostete Zone für die untergeordnete Subdomäne erstellen möchten, erstellen Sie den NS-Datensatz für die untergeordnete Subdomäne in der gehosteten Zone für die Subdomäne, die eine Ebene näher am Domänennamen liegt. Auf diese Weise können Sie sicherstellen, dass der Datenverkehr ordnungsgemäß an Ihre Ressourcen weitergeleitet wird. Angenommen, Sie möchten Datenverkehr für die folgenden Subdomänen weiterleiten:

- subdomain1.example.com
- subdomain2.subdomain1.example.com

Um eine andere gehostete Zone zur Weiterleitung des Datenverkehrs für subdomain2.subdomain1.example.com zu verwenden, gehen Sie wie folgt vor:

1. Erstellen Sie eine gehostete Zone mit dem Namen subdomain2.subdomain1.example.com.
2. Erstellen Sie Datensätze in der gehosteten Zone subdomain2.subdomain1.example.com. Weitere Informationen finden Sie unter Erstellen von Datensätzen in der gehosteten Zone für die Subdomäne.
3. Kopieren Sie die Namen der Namensserver für die gehostete Zone subdomain2.subdomain1.example.com.
4. Erstellen Sie in der gehosteten Zone subdomain1.example.com einen NS-Datensatz namens subdomain2.subdomain1.example.com und fügen Sie die Namen der Namensserver für die gehostete Zone subdomain2.subdomain1.example.com ein.

Löschen Sie außerdem alle doppelten Datensätze aus der Subdomäne1.example.com. Weitere Informationen finden Sie unter Aktualisieren der gehosteten Zone für die Domäne.

Nachdem Sie diesen NS-Datensatz erstellt haben, verwendet Route 53 die gehostete Zone subdomain2.subdomain1.example.com, um den Datenverkehr für die Subdomäne subdomain2.subdomain1.example.com weiterzuleiten.

Arbeiten mit gehosteten Zonen

Eine gehostete Zone ist ein Container für Datensätze. Diese Datensätze enthalten Informationen darüber, wie Sie Datenverkehr zu einer bestimmten Domäne (z. B. example.com) und ihren Unterdomänen (z. B. acme.example.com, zenith.example.com) weiterleiten wollen. Eine gehostete Zone trägt denselben Namen wie die entsprechende Domäne. Es gibt zwei Arten von Hosting-Zonen:

- Öffentliche gehostete Zonen enthalten Datensätze, die angeben, wie Sie Datenverkehr im Internet weiterleiten wollen. Weitere Informationen finden Sie unter Arbeiten mit öffentlichen gehosteten Zonen.
- Private gehostete Zonen enthalten Datensätze, die angeben, wie Sie Datenverkehr in einer Amazon VPC weiterleiten wollen. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.

Arbeiten mit öffentlichen gehosteten Zonen

Eine öffentliche gehostete Zone ist ein Container mit Informationen darüber, wie Sie im Internet Datenverkehr zu einer bestimmten Domäne (z. B. example.com) und ihren Unterdomänen (z. B. acme.example.com, zenith.example.com) weiterleiten wollen. Sie erhalten eine öffentliche gehostete Zone auf eine von zwei Arten:

- Wenn Sie eine Domäne bei Route 53 registrieren, erstellen wir für Sie automatisch eine gehostete Zone.
- Bei der Übertragung von DNS-Dienst für eine vorhandene Domäne nach Route 53 erstellen Sie zuerst eine gehostete Zone für die Domäne. Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

In beiden Fällen erstellen Sie anschließend Datensätze in der gehosteten Zone, um anzugeben, wie der Datenverkehr für die Domäne und die Unterdomänen weitergeleitet werden soll. Sie können

beispielsweise einen Datensatz erstellen, um den Verkehr für www.example.com an eine CloudFront Distribution oder einen Webserver in Ihrem Rechenzentrum weiterzuleiten. Weitere Informationen über Einträge finden Sie unter Arbeiten mit Datensätzen.

In diesem Thema wird erläutert, wie Sie die Amazon Route 53-Konsole verwenden, um öffentlich gehostete Zonen zu erstellen, aufzulisten und zu löschen.

> **Note**
>
> Sie können auch eine privat gehostete Route 53-Zone verwenden, um den Verkehr innerhalb einer oder mehrerer Zonen weiterzuleiten VPCs , die Sie mit dem Amazon VPC-Service erstellen. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.

Themen

Überlegungen zum Arbeiten mit öffentlichen gehosteten Zonen

Beachten Sie die folgenden Überlegungen, wenn Sie mit öffentlichen gehosteten Zonen arbeiten:

NS- und SOA-Datensätze

Bei der Erstellung einer gehosteten Zone erstellt Amazon Route 53 automatisch einen NS-Eintrag (Namenserver) und einen SOA-Eintrag (Start of Authority, Autoritätsursprung) für die Zone. Der NS-Eintrag identifiziert die vier Namenserver, die Sie der Vergabestelle oder dem DNS-Dienst nennen, sodass DNS-Abfragen an die Route 53-Namenserver weitergeleitet werden.

Weitere Informationen über NS- und SOA-Einträge finden Sie unter NS- und SOA-Datensätze, die Amazon Route 53 für eine öffentliche gehostete Zone erstellt.

Mehrere gehostete Zonen mit demselben Namen

Sie können mehr als eine gehostete Zone mit demselben Namen erstellen und verschiedene Datensätze für jede gehostete Zone hinzufügen. Route 53 weist jeder gehosteten Zone vier Nameserver zum, und die Nameserver sind jeweils unterschiedlich. Wenn Sie die Nameserverdatensätze Ihrer Vergabestellt ändern, achten Sie darauf, Route 53-Nameserver für die richtige gehostete Zone verwenden, nämlich die mit den Ressourcendatensätze, die Route 53 für die Antwort auf Abfragen für Ihre Domäne verwenden soll. Route 53 gibt nie Werte für Datensätze in anderen gehosteten Zonen aus, die denselben Namen haben.

Wiederverwendbare Delegationssätze

Standardmäßig weist Route 53 einen eindeutigen Satz von vier Nameservern (gemeinsam Delegierungsgruppe genannt) jeder gehosteten Zone zu, die Sie erstellen. Wenn Sie eine große Anzahl von gehosteten Zonen erstellen möchten, können Sie programmgesteuert eine wiederverwendbare Delegierungsgruppe erstellen. (Wiederverwendbare Delegierungsgruppen sind nicht in der Route 53-Konsole verfügbar.) Anschließend können Sie gehostete Zonen programmgesteuert erstellen und jeder gehostete Zone dieselbe wiederverwendbare Delegierungsgruppe zuordnen – dieselben vier Namenserver.

Wiederverwendbare Delegierungsgruppen vereinfachen die Migration des DNS-Dienst in Route 53, da Sie Ihre Domänenname-Vergabestelle anweisen können, dieselben vier Namenserver für alle Domänen zu verwenden, für die Route 53 als DNS-Dienst verwendet werden soll. Weitere Informationen finden Sie CreateReusableDelegationSetin der Amazon Route 53 API-Referenz.

Erstellen einer öffentlichen gehosteten Zone

Eine öffentliche gehostete Zone ist ein Container mit Informationen darüber, wie Sie im Internet Datenverkehr zu einer bestimmten Domäne (z. B. example.com) und ihren Unterdomänen (z. B. acme.example.com, zenith.example.com) weiterleiten wollen. Nachdem Sie eine gehostete Zone erstellt haben, legen Sie Datensätze an, um anzugeben, wie der Datenverkehr für die Domäne und die Unterdomänen weitergeleitet werden soll.

⚠ Einschränkungen

Beachten Sie die folgenden Einschränkungen für die Erstellung von Hosting-Zonen mit Route 53.

- Sie können eine gehostete Zone nur für eine Domäne erstellen, die Sie über die Berechtigung zur Verwaltung verfügen. Das heißt in der Regel, dass Sie Eigentümer der Domäne sind. Es könnte aber auch bedeuten, dass Sie eine Anwendung für den Eigentümer entwickeln.
- Sie können Hosting-Zonen nur für Domains und Subdomains erstellen. Route 53 unterstützt nicht das Hosten von Top-Level-Domains (TLD) wie. `.com`

So erstellen Sie eine öffentlich gehostete Zone mit der Route 53-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wenn Sie erst mit der Verwendung von Route 53 begonnen haben, wählen Sie Get Started (Erste Schritte) unter DNS Management aus.

   Wenn Sie Route 53 bereits nutzen, wählen Sie Hosted zones (Gehostete Zonen) im Navigationsbereich aus.
3. Wählen Sie Create Hosted Zone (Gehostete Zone) aus.
4. Geben Sie im Bereich Create Hosted Zone (Gehostete Zone erstellen) den Namen der Domäne ein, zu der Sie Datenverkehr weiterleiten wollen. Optional können Sie auch einen Kommentar eingeben.

   Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.
5. Übernehmen Sie für Type (Typ) den Standardwert Public Hosted Zone (Öffentlich gehostete Zone).
6. Wählen Sie Erstellen aus.
7. Erstellen Sie Datensätze, die angeben, wie Sie den Datenverkehr für die Domäne und die Unterdomänen weiterleiten möchten. Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

8. Informationen zur Verwendung von Datensätzen in der neuen gehosteten Zone zur Weiterleitung des Datenverkehrs für Ihre Domäne finden Sie unter dem entsprechenden Thema:

   - Wenn Sie Route 53 als DNS-Dienst für eine Domäne verwenden, die bei einer anderen Domänenvergabestelle registriert ist, lesen Sie nach unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.
   - Wenn die Domäne mit Route 53 registriert wurde, lesen Sie Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Das Abrufen der Nameserver für eine öffentliche gehostete Zone

Sie erhalten die Nameserver für eine öffentliche gehostete Zone, wenn Sie den DNS-Dienst für Ihre Domänenregistrierung ändern möchten. Informationen zum Ändern des DNS-Dienstes finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

> **Note**
>
> Bei einigen Vergabestellen ist die Angabe von vollständig qualifizierten Domänennamen unzulässig. Dort können Sie Namenserver nur unter Verwendung von IP-Adressen angeben. Wenn Ihre Vergabestelle voraussetzt, dass Sie IP-Adressen verwenden, können Sie die IP-Adressen für Ihre Namensserver mithilfe von "dig" (für Mac, Unix oder Linux) oder "nslookup" (für Windows) abrufen. Wir ändern die IP-Adressen von Namensservern selten. Wenn wir die IP-Adressen ändern müssen, benachrichtigen wir Sie im Voraus.

So rufen Sie die Nameserver für eine gehostete Zone mithilfe der Route 53-Konsole ab

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone aus und wählen Sie dann View Details (Details anzeigen) aus.
4. Wählen Sie auf der Detailseite für die gehostete Zone Hosted Zone details (Details der gehosteten Zone) aus.
5. Notieren Sie sich die vier Namen, die für Name Servers aufgelistet werden.

Auflisten der öffentlichen gehosteten Zonen

Sie können die Amazon Route 53-Konsole verwenden, um alle Hosting-Zonen aufzulisten, die Sie mit dem aktuellen AWS Konto erstellt haben. Informationen zum Auflisten von Hosting-Zonen mithilfe der Route 53-API finden Sie ListHostedZonesin der Amazon Route 53-API-Referenz.

So listen Sie mithilfe der Route 53-Konsole die öffentlichen Hosting-Zonen auf, die einem AWS Konto zugeordnet sind

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen). Auf der Seite wird eine Liste der Hosting-Zonen angezeigt, die dem AWS Konto zugeordnet sind, mit dem Sie derzeit angemeldet sind.
3. Verwenden Sie die Suchleiste oben in der Tabelle, um gehostete Zonen zu filtern.

   Das Suchverhalten hängt davon ab, ob die gehostete Zone bis zu 2.000 Datensätze oder mehr als 2.000 Datensätze enthält:

   Bis zu 2.000 gehostete Zonen

   - Um Datensätze anzuzeigen, die einen bestimmten Wert haben, klicken Sie auf die Suchleiste, wählen Sie eine Eigenschaft in der Dropdown-Liste aus, und geben Sie einen Wert ein. Sie können einen Wert auch direkt in der Suchleiste eingeben und die Eingabetaste drücken. Um beispielsweise die gehosteten Zonen anzuzeigen, die einen Namen haben, der mit**abc**Geben Sie diesen Wert in die Suchleiste ein und drücken Sie die Eingabetaste.
   - Um nur die gehosteten Zonen anzuzeigen, die denselben gehosteten Zonentyp haben, wählen Sie den Typ in der Dropdown-Liste aus, und geben Sie den Typ ein.

   Mehr als 2.000 gehostete Zonen

   - Sie können nach Eigenschaften basierend auf dem genauen Domänennamen, allen Eigenschaften und dem Typ suchen.
   - Suchen Sie mit dem genauen Domainnamen für schnellere Suchergebnisse.

Anzeigen von DNS-Abfragemetriken für eine öffentliche gehostete Zone

Sie können die Gesamtzahl der DNS-Abfragen anzeigen, die Route 53 für eine bestimmte öffentliche gehostete Zone oder eine Kombination aus öffentlichen gehosteten Zonen beantwortet. Die Metriken werden in angezeigt CloudWatch, sodass Sie ein Diagramm anzeigen, den Zeitraum auswählen können, den Sie anzeigen möchten, und die Metriken auf eine Vielzahl anderer Arten anpassen können. Sie können auch Alarme erstellen und Benachrichtigungen konfigurieren, sodass Sie benachrichtigt werden, wenn die Anzahl der DNS-Abfragen in einem bestimmten Zeitraum ein bestimmtes Level über- oder unterschreitet.

> **Note**
>
> Route 53 sendet automatisch die Anzahl der DNS-Abfragen an CloudWatch alle öffentlich gehosteten Zonen, sodass Sie nichts konfigurieren müssen, bevor Sie die Abfragemetriken anzeigen können. Für DNS-Abfragemetriken fallen keine Gebühren an.

Welche DNS-Abfragen werden gezählt?

Metriken enthalten nur die Abfragen, die DNS-Resolver an Route 53 weiterleiten. Wenn ein DNS-Auflöser die Antwort auf eine Abfrage (z. B. die IP-Adresse für einen Load Balancer für example.com) bereits zwischengespeichert hat, gibt der Auflöser die zwischengespeicherte Antwort weiter zurück, ohne die Abfrage an Route 53 weiterzuleiten, bis die TTL für den entsprechenden Datensatz abgelaufen ist.

Abhängig davon, wie viele DNS-Abfragen für einen Domänennamen (example.com) oder Subdomänennamen (www.example.com) übermittelt werden, welche Resolver von Ihren Benutzern verwendet werden und welche TTL für den Datensatz gilt, enthalten die DNS-Abfragemetriken möglicherweise Informationen zu nur einer von mehreren tausend Abfragen, die an DNS-Resolver übermittelt wurden. Weitere Information zur Funktionsweise von DNS finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wann werden Abfragemetriken für eine gehostete Zone in CloudWatch angezeigt?

Nachdem Sie eine gehostete Zone erstellt haben, kommt es zu einer Verzögerung von bis zu mehreren Stunden, bevor die gehostete Zone in CloudWatch angezeigt werden kann. Darüber hinaus müssen Sie eine DNS-Abfrage für einen Datensatz in der gehosteten Zone senden, damit Daten angezeigt werden können.

Abrufen von Metriken sind nur in USA Ost (Nord-Virginia) verfügbar

Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben. Um Metriken mit der AWS CLI abzurufen, müssen Sie die AWS Region entweder nicht spezifizieren oder `us-east-1` als Region angeben. Route 53 Metriken sind nicht verfügbar, wenn Sie eine andere Region auswählen.

CloudWatch Metrik und Dimension für DNS-Abfragen

Informationen zur CloudWatch Metrik und Dimension für DNS-Abfragen finden Sie unterÜberwachung von Hosting-Zonen mit Amazon CloudWatch. Informationen zu CloudWatch Metriken finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Anfordern detaillierterer Daten zu DNS-Abfragen

Um detailliertere Informationen zu jeder DNS-Abfrage zu erhalten, die Route 53 beantwortet, einschließlich der folgenden Werte, können Sie die Abfrageprotokollierung konfigurieren:

- Domain oder Subdomain, die angefordert wurde
- Das Datum und die Uhrzeit der Anforderung
- DNS-Datensatztyp (z. B. A oder AAAA)
- Der Edge-Standort von Route 53, der auf die DNS-Abfrage geantwortet hat
- Der DNS-Antwortcode, wie z. B. `NoError` oder `ServFail`

Weitere Informationen finden Sie unter Öffentliche DNS-Abfrageprotokollierung.

So erhalten Sie DNS-Abfragemetriken

Kurz nachdem Sie eine gehostete Zone erstellt haben, beginnt Amazon Route 53, Metriken und Dimensionen einmal pro Minute an zu senden CloudWatch. Sie können die folgenden Verfahren verwenden, um die Metriken auf der CloudWatch Konsole oder mithilfe von AWS Command Line Interface (AWS CLI) anzuzeigen.

Themen

- DNS-Abfragemetriken für eine öffentlich gehostete Zone in der CloudWatch Konsole anzeigen
- Abrufen von DNS-Abfragemetriken mithilfe der AWS CLI

DNS-Abfragemetriken für eine öffentlich gehostete Zone in der CloudWatch Konsole anzeigen

Gehen Sie wie folgt vor, um DNS-Abfragemetriken für öffentlich gehostete Zonen in der CloudWatch Konsole anzuzeigen.

Um DNS-Abfragemetriken für eine öffentlich gehostete Zone auf der CloudWatch Konsole anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie in der Liste der AWS Regionen in der oberen rechten Ecke der Konsole die Option USA Ost (Nord-Virginia) aus. Route 53-Metriken sind nicht verfügbar, wenn Sie eine andere AWS Region auswählen.
4. Klicken Sie auf der Registerkarte All metrics auf Route 53.
5. Wählen Sie Hosted Zone Metrics (Metriken für gehostete Zonen) aus.
6. Aktivieren Sie das Kontrollkästchen für eine oder mehrere Hosting-Zonen, die den Metriknamen haben DNSQueries.
7. Ändern Sie auf der Registerkarte Graphed metrics (Grafische Metriken) die entsprechenden Werte, um die Metriken im gewünschten Format anzuzeigen.

   Wählen Sie für Statistik die Option Summe oder SampleCount; beide Statistiken zeigen denselben Wert an.

Abrufen von DNS-Abfragemetriken mithilfe der AWS CLI

Um DNS-Abfragemetriken mit dem AWS CLI abzurufen, verwenden Sie den get-metric-dataBefehl. Beachten Sie Folgendes:

- Sie geben die meisten Werte für den Befehl in einer separaten JSON-Datei an. Weitere Informationen finden Sie unter get-metric-data.
- Der Befehl gibt einen Wert für jedes Intervall zurück, das Sie für `Period` in der JSON-Datei angeben. `Period` wird in Sekunden angegeben. Wenn Sie also einen Zeitraum von fünf Minuten und `60` für `Period` angeben, erhalten Sie fünf Werte. Wenn Sie einen Zeitraum von fünf Minuten und `300` für `Period` angeben, erhalten Sie einen Wert.
- In der JSON-Datei können Sie einen beliebigen Wert für `Id` angeben.

- Lassen Sie die AWS Region entweder unspezifiziert oder geben Sie `us-east-1` sie als Region an. Route 53 Metriken sind nicht verfügbar, wenn Sie eine andere Region auswählen. Weitere Informationen finden Sie unter Konfiguration der AWS CLI im AWS Command Line Interface Benutzerhandbuch.

Hier ist der AWS CLI Befehl, mit dem Sie DNS-Abfragemetriken für den Zeitraum von fünf Minuten zwischen 4:01 und 4:07 Uhr am 1. Mai 2019 abrufen. Der `metric-data-queries`-Parameter verweist auf die JSON-Beispieldatei, die dem Befehl folgt.

```
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
```

Hier sehen Sie die Beispiel-JSON-Datei:

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

Hier sehen Sie die Ausgabe dieses Befehls. Beachten Sie Folgendes:

- Die Start- und Endzeit im Befehl decken einen Zeitraum von sieben Minuten ab, `2019-05-01T04:01:00Z` bis `2019-05-01T04:07:00Z`.

- Es gibt nur sechs Rückgabewerte. Es gibt keinen Wert für `2019-05-01T04:05:00Z`, da während dieser Minute keine DNS-Abfragen stattgefunden haben.
- Der in der JSON-Datei `Period` angegebene Wert ist `60` (Sekunden), sodass die Werte in 1-Minuten-Intervallen gemeldet werden.

```
{
    "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"
            ]
        }
    ]
}
```

Löschen einer öffentlichen gehosteten Zone

In diesem Abschnitt wird erläutert, wie Sie eine öffentlich gehostete Zone mithilfe der Amazon-Route-53-Konsole verwenden können.

Sie können eine gehostete Zone nur dann löschen, wenn keine Datensätze (abgesehen von den Standard-SOA- und NS-Datensätzen) vorhanden sind. Wenn Ihre gehostet Zone andere Datensätze enthält, müssen Sie diese löschen, bevor Sie Ihre gehostete Zone löschen können. Dadurch wird verhindert, dass Sie versehentlich eine gehostete Zone löschen, die noch Datensätze enthält.

Themen

Verhindern einer Weiterleitung des Datenverkehrs zu Ihrer Domäne

Wenn Sie Ihre Domänenregistrierung behalten möchten, aber die Weiterleitung von Internetdatenverkehr an Ihre Website oder Webanwendung beenden möchten, empfehlen wir, dass Sie Datensätze in der gehosteten Zone löschen, statt die gehostete Zone zu löschen.

> **Important**
>
> Wenn Sie eine gehostete Zone löschen, können Sie diese nicht wiederherstellen. Sie müssen eine neue gehostete Zone erstellen und Sie die Namensserver für Ihre Domain-Registrierung aktualisieren. Es kann bis zu 48 Stunden dauern, bis diese Einstellungen wirksam werden. Wenn Sie eine gehostete Zone löschen, könnte sich außerdem jemand die Domäne aneignen und den Datenverkehr über Ihren Domänennamen an die eigenen Ressourcen weiterleiten.
>
> Wenn Sie die Zuständigkeit für eine Subdomäne an eine gehostete Zone delegiert haben und die untergeordnete gehostete Zone löschen möchten, müssen Sie auch die übergeordnete gehostete Zone aktualisieren. Löschen Sie hierzu den NS-Datensatz, der denselben Namen wie die untergeordnete gehostete Zone hat. Wenn Sie z. B. die gehostete Zone „acme.example.com“ löschen möchten, müssen Sie auch den NS-Datensatz „acme.example.com“ in der gehosteten Zone „example.com“ löschen. Es wird empfohlen, zuerst den NS-Datensatz zu löschen und auf die Dauer der TTL für den NS-Datensatz zu warten, bevor Sie die untergeordnete gehostete Zone löschen. Dadurch wird sichergestellt, dass sich niemand die untergeordnete gehostete Zone aneignen kann, während die Nameserver für die untergeordnete gehostete Zone noch in DNS-Resolvern zwischengespeichert sind.

Wenn Sie die monatliche Gebühr für die gehostete Zone vermeiden möchten, können Sie den DNS-Dienst für die Domäne auf einen kostenlosen DNS-Dienst übertragen. Wenn Sie den DNS-Dienst übertragen, müssen Sie die Nameserver für die Domänenregistrierung aktualisieren. Wenn die Domäne bei Route 53 registriert ist, finden Sie unter Hinzufügen oder Ändern der Nameserver und

Glue-Datensätze in einer Domäne Informationen darüber, wie Sie Route 53-Nameserver durch Nameserver für den neuen DNS-Dienst ersetzen können. Wenn die Domäne mit einer anderen Vergabestellt registriert wurde, verwenden Sie die Methode der Vergabestelle, um Namensserver für die Domänenregistrierung zu aktualisieren. Weitere Informationen finden Sie über eine Internet-Suche nach „kostenloser DNS-Dienst“.

Löschen von öffentlichen gehosteten Zonen, die von einem anderen Dienst erstellt wurden

Wenn eine gehostete Zone von einem anderen Dienst erstellt wurde, können Sie diese nicht mithilfe der Route 53-Konsole löschen. Stattdessen müssen Sie den entsprechenden Vorgang für den anderen Dienst verwenden:

- AWS Cloud Map— Um eine gehostete Zone zu löschen, die bei der AWS Cloud Map Erstellung eines öffentlichen DNS-Namespace erstellt wurde, löschen Sie den Namespace. AWS Cloud Map löscht die gehostete Zone automatisch. Weitere Informationen finden Sie unter Löschen von Namespaces im AWS Cloud Map Entwicklerleitfaden.
- Amazon Elastic Container Service (Amazon ECS) Service Discovery - So löschen Sie eine öffentlich gehostete Zone, die Amazon ECS erstellt hat, als Sie einen Dienst mithilfe der Dienst-Erkennung erstellt haben, löschen Sie die Amazon-ECS-Dienste, die den Namespace verwenden und löschen Sie den Namespace. Weitere Informationen finden Sie unter Angeben vertraulicher Daten im Amazon Elastic Container Service-Entwicklerleitfaden.

Löschen einer öffentlichen gehosteten Zone mit der Route 53-Konsole.

Um die Route 53-Konsole zu verwenden, um eine öffentlich gehostete Zone zu löschen, führen Sie folgendes Verfahren durch.

Löschen einer öffentlichen gehosteten Zone mit der Route 53-Konsole.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Gehostete Zonen aus und wählen Sie den hervorgehobenen Link für die gehostete Zone aus, die Sie löschen möchten.
3. Vergewissern Sie sich, dass die gehostete Zone, die Sie löschen möchten, nur einen NS- und einen SOA-Datensatz enthält. Enthält sie zusätzliche Datensätze, löschen Sie diese. Sie müssen auch die DNSSEC-Signierung deaktivieren:

> **Note**
>
> Wenn Sie versuchen, die gehostete Zone zu löschen, ohne diese Anforderungen zu erfüllen, gibt Route 53 einen Fehler zurück:
>
> - Wenn die DNSSEC-Signatur aktiviert ist: Die angegebene Hosting-Zone enthält DNSSEC-Schlüssel zur Schlüsselsignatur und kann daher nicht gelöscht werden
> - Falls andere Ressourcendatensätze existieren (außer den standardmäßigen SOA- und NS-Datensätzen): Die angegebene Hosting-Zone enthält nicht erforderliche Ressourcendatensätze und kann daher nicht gelöscht werden

- Klicken Sie auf der Detailseite für die gehostete Zone in der Liste Records (Datensätze), wenn die Liste der Datensätze irgendwelche Datensätze enthält, für die der Wert der Spalte Type (Typ) ein anderer ist als NS oder SOA, auf die entsprechende Zeile, und wählen Sie Delete (Löschen) aus.

  Um mehrere aufeinander folgende Datensätze auszuwählen, wählen Sie die erste Zeile aus, halten Sie die Umschalttaste gedrückt, und klicken Sie dann auf die letzte Zeile. Um mehrere nicht aufeinander folgende Datensätze auszuwählen, wählen Sie die erste Zeile aus, halten Sie die Strg-Taste gedrückt, und klicken Sie dann auf die gewünschten Zeilen.

  > **Note**
  >
  > Wenn Sie NS-Datensätze für Subdomänen in der gehosteten Zone erstellt haben, löschen Sie auch diese Datensätze.

4. Navigieren Sie zurück auf die Seite Hosted Zones (Gehostete Zonen) und wählen Sie die Zeile für die gehostete Zone aus, die Sie löschen möchten.
5. Wählen Sie Löschen aus.
6. Geben Sie den Bestätigungsschlüssel ein und wählen Sie Delete (Löschen) aus.
7. Wenn Sie möchten, dass die Domäne im Internet nicht verfügbar ist, empfehlen wir Ihnen, den DNS-Dienst auf einen kostenlosen DNS-Dienst zu übertragen und dann die in Route 53 gehostete Zone zu löschen. Dadurch wird verhindert, dass zukünftige DNS-Abfragen möglicherweise fehlgeleitet werden.

Wenn die Domäne bei Route 53 registriert ist, finden Sie unter Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne Informationen darüber, wie Sie Route 53-Nameserver durch Nameserver für den neuen DNS-Dienst ersetzen können. Wenn die Domäne mit einer anderen Vergabestellt registriert wurde, verwenden Sie die Methode der Vergabestelle, um Namensserver für die Domäne zu ändern.

> **Note**
>
> Wenn Sie eine gehostete Zone für eine Subdomäne (acme.example.com) löschen, müssen Sie keine Namensserver für die Domäne (example.com) ändern.

Überprüfen der DNS-Antworten von Route 53

Wenn Sie eine gehostete Amazon Route 53-Zone für Ihre Domain erstellt haben, können Sie die DNS-Überprüfung in der Konsole verwenden, um zu sehen, wie Route 53 auf DNS-Abfragen antwortet, wenn Sie Ihre Domain so konfigurieren, dass sie Route 53 als DNS-Dienst verwendet. Für Daten zu Geolokalisierung, Geonähe und Latenz können Sie auch Abfragen von einer bestimmten and/or Client-IP-Adresse des DNS-Resolver-Clients simulieren, um herauszufinden, welche Antwort Route 53 zurückgeben würde.

> **Important**
>
> Das Tool sendet keine Abfragen an das Domain Name System. Es antwortet nur basierend auf den Einstellungen in den Datensätzen in der gehosteten Zone. Das Tool gibt unabhängig davon, ob die gehostete Zone derzeit verwendet wird dieselben Informationen zurück, um Datenverkehr für die Domäne weiterzuleiten.

Die DNS-Überprüfung funktioniert nur bei öffentlichen gehosteten Zonen.

> **Note**
>
> Das DNS-Prüftool gibt ähnliche Informationen zurück wie im Antwortabschnitt des Befehls `dig`. Wenn Sie also die Namenserver einer Unterdomain abfragen, die auf die übergeordneten Namenserver verweisen, werden diese nicht zurückgegeben.

Themen

Mit der Überprüfung die Antworten von Amazon Route 53 auf DNS-Abfragen anzeigen

Sie können das Tool verwenden, um zu sehen, welche Antwort Amazon Route 53 als Antwort auf eine DNS-Abfrage für einen Datensatz gibt.

So sehen Sie anhand der Überprüfung, wie Route 53 auf DNS-Abfragen reagiert

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Hosted Zones.
3. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) den Namen der gehosteten Zone aus. Auf der Konsole wird die Liste der Datensätze für diese gehostete Zone angezeigt.
4. Um direkt zur Seite Check response from Route 53 zu gelangen, wählen Sie Test record set.
5. Geben Sie die folgenden Werte an:

   - Der Name des Datensatzes, abgesehen vom Namen der gehosteten Zone. Um beispielsweise www.example.com, zu überprüfen, geben Sie www ein. Um example.com zu überprüfen, lassen Sie das Feld Record name (Datensatzname) leer.
   - Der Typ des Datensatzes, den Sie überprüfen möchten, z. B. A oder CNAME.
6. Wählen Sie Get Response (Antwort abrufen).
7. Der Abschnitt Response returned by Route 53 enthält die folgenden Werte:

   DNS-Antwortcode

   Ein Code, der angibt, ob die Abfrage gültig war oder nicht. Der gängigste Antwortcode ist NOERROR und bedeutet, dass die Abfrage gültig war. Wenn die Antwort nicht gültig ist, gibt Route 53 einen Antwortcode mit Erklärung aus. Eine Liste der möglichen Antwortcodes finden Sie unter DNS RCODES auf der IANA-Website.

   Protocol (Protokoll)

   Das Protokoll, das Amazon Route 53 für die Beantwortung einer Abfrage verwendet hat, entweder UDP oder TCP.

Von Route 53 zurückgegebene Antwort

Der Wert, den Route 53 an eine Webanwendung zurückgeben würde. Der Wert ist einer der folgenden:

- Bei Nicht-Alias-Datensätzen enthält die Antwort den Wert oder die Werte im Datensatz.
- Bei mehreren Datensätzen, die denselben Namen und Typ haben, der Gewichtung, Latenz, Geolokation und Failover beinhaltet, enthält die Antwort den Wert aus dem entsprechenden Datensatz und basierend auf der Anforderung.
- Bei Aliaseinträgen, die auf andere AWS Ressourcen als einen anderen Datensatz verweisen, enthält die Antwort je nach AWS Ressourcentyp eine IP-Adresse oder einen Domänennamen für die Ressource.
- Bei Alias-Datensätzen, die auf andere Datensätze verweisen, enthält die Antwort den/die Wert(e) aus dem referenzierten Datensatz.

Verwendung der Überprüfung zur Simulation von Abfragen von spezifischen IP-Adressen (nur Datensätze für Geolokation und Latenz)

Wenn Sie Datensätze für Latenz oder Geolokation erstellt haben, können Sie das Überprüfungstool verwenden, um Abfragen von der IP-Adresse für einen DNS-Resolver und einen Client zu simulieren.

So verwenden Sie die Überprüfung zur Simulation von Abfragen von angegebenen IP-Adressen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones.
3. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) den Namen der gehosteten Zone aus. Auf der Konsole wird die Liste der Datensätze für diese gehostete Zone angezeigt.
4. Um direkt zur Seite Check response from Route 53 zu gelangen, wählen Sie Test record set.

   Um zur Seite Check response from Route 53 für einen bestimmten Datensatz zu gelangen, markieren Sie das Kontrollkästchen für den entsprechenden Datensatz, und wählen Sie dann Test record set.
5. Wenn Sie Test record set (Datensatz testen) ausgewählt haben, ohne vorher einen Datensatz auszuwählen, geben Sie die folgenden Werte an:

- Der Name des Datensatzes, abgesehen vom Namen der gehosteten Zone. Um beispielsweise www.example.com, zu überprüfen, geben Sie www ein. Um example.com zu überprüfen, lassen Sie das Feld Record name (Datensatzname) leer.
- Der Typ des Datensatzes, den Sie überprüfen möchten, z. B. A oder CNAME.

6. Geben Sie die anwendbaren Werte an:

   Resolver-IP-Adresse

   Geben Sie eine IPv4 IPv6 Oder-Adresse an, um den Standort des DNS-Resolvers zu simulieren, den ein Client für Anfragen verwendet. Dies ist für das Testen von Datensätzen für Latenz und Geolokation hilfreich. Wenn Sie diesen Wert weglassen, verwendet das Tool die IP-Adresse eines DNS-Resolvers in der Region AWS USA Ost (Nord-Virginia) (us-east-1).

   EDNS0-Client-Subnetz-IP

   Wenn der Resolver EDNS0 unterstützt, geben Sie die Client-Subnetz-IP für eine IP-Adresse an der jeweiligen Geolokation ein, z. B. 192.0.2.0 oder 2001:db8:85a3::8a2e:370:7334.

   Subnetzmaske

   Wenn Sie für EDNS0 client subnet IP eine IP-Adresse angeben, können Sie optional die Anzahl Bits für die IP-Adresse angeben, welche die Überprüfung bei der DNS-Abfrage berücksichtigen soll. Wenn Sie z. B. 192.0.2.44 für EDNS0 client subnet IP und 24 für Subnet mask angeben, simuliert die Überprüfung eine Abfrage von 192.0.2.0/24. Der Standardwert ist 24 Bit für IPv4 Adressen und 64 Bit für Adressen. IPv6

7. Wählen Sie Get Response (Antwort abrufen).
8. Der Abschnitt Response returned by Route 53 enthält die folgenden Werte:

   An Route 53 gesendete DNS-Abfrage

   Die Abfrage im BIND format, welche die Überprüfung an Route 53 gesendet hat. Dies ist dasselbe Format, das eine Webanwendung zum Senden einer Abfrage verwenden würde. Diese drei Werte sind typischerweise der Name des Datensatzes, IN (für Internet) und der Typ des Datensatzes.

   DNS-Antwortcode

   Ein Code, der angibt, ob die Abfrage gültig war oder nicht. Der gängigste Antwortcode ist NOERROR und bedeutet, dass die Abfrage gültig war. Wenn die Antwort nicht gültig ist, gibt

Route 53 einen Antwortcode mit Erklärung aus. Eine Liste der möglichen Antwortcodes finden Sie unter DNS RCODES auf der IANA-Website.

Protocol (Protokoll)

Das Protokoll, das Amazon Route 53 für die Beantwortung einer Abfrage verwendet hat, entweder UDP oder TCP.

Von Route 53 zurückgegebene Antwort

Der Wert, den Route 53 an eine Webanwendung zurückgeben würde. Der Wert ist einer der folgenden:

- Bei Nicht-Alias-Datensätzen enthält die Antwort den Wert oder die Werte im Datensatz.
- Bei mehreren Datensätzen, die denselben Namen und Typ haben, der Gewichtung, Latenz, Geolokation und Failover beinhaltet, enthält die Antwort den Wert aus dem entsprechenden Datensatz und basierend auf der Anforderung.
- Bei Aliaseinträgen, die auf andere AWS Ressourcen als einen anderen Datensatz verweisen, enthält die Antwort je nach AWS Ressourcentyp eine IP-Adresse oder einen Domänennamen für die Ressource.
- Bei Alias-Datensätzen, die auf andere Datensätze verweisen, enthält die Antwort den/die Wert(e) aus dem referenzierten Datensatz.

Konfigurieren von White-Label-Nameservern

Jede gehostete Amazon Route 53-Zone ist mit vier Namenservern verknüpft, die zusammen als Delegierungsgruppe bezeichnet werden. Standardmäßig haben die Nameserver Namen wie ns-2048.awsdns-64.com. Wenn der Domänenname Ihrer Nameserver derselbe sein soll wie der Domänenname Ihrer gehosteten Zone, beispielsweise ns1.example.com, können Sie die White-Label-Nameserver (auch Vanity-Nameserver oder private Nameserver genannt) konfigurieren.

In den folgenden Schritten wird erläutert, wie Sie eine Gruppe von vier White-Label-Nameservern so konfigurieren, dass Sie sie für mehrere Domänen wiederverwenden können. Angenommen, Sie besitzen die Domänen example.com, example.org und example.net. Mit diesen Schritten können Sie White-Label-Nameserver für example.com konfigurieren und für example.org und example.net wiederverwenden.

Themen

- Schritt 1: Erstellen einer wiederverwendbaren Route 53-Delegierungsgruppe

- Schritt 2: Erstellen oder Neuerstellen von gehosteten Amazon Route 53-Zonen und Ändern der TTL für NS- und SOA-Datensätze
- Schritt 3: Erneutes Erstellen von Datensätzen für Ihre gehosteten Zonen
- Schritt 4: IP-Adressen abrufen
- Schritt 5: Erstellen von Datensätzen für White-Label-Nameserver
- Schritt 6: Aktualisieren der NS- und SOA-Datensätze
- Schritt 7: Erstellen und Ändern der Nameserver der Vergabestelle
- Schritt 8: Überwachen des Datenverkehrs für die Website oder Anwendung
- Schritt 9: Kehren Sie zu den ursprünglichen Werten TTLs zurück
- Schritt 10: Kontaktieren von rekursiven DNS-Dienstes (optional)

Schritt 1: Erstellen einer wiederverwendbaren Route 53-Delegierungsgruppe

White-Label-Name-Server sind einem wiederverwendbaren Route 53-Delegierungssatz zugeordnet. Sie können White-Label-Nameserver nur dann für eine gehostete Zone verwenden, wenn die gehostete Zone und der wiederverwendbare Delegierungssatz von demselben AWS Konto erstellt wurden.

Um einen wiederverwendbaren Delegierungssatz zu erstellen, können Sie die Route 53-API, die AWS CLI oder eine der folgenden verwenden AWS SDKs. Weitere Informationen finden Sie in der folgenden Dokumentation:

- Route 53-API — Weitere Informationen finden Sie CreateReusableDelegationSetin der Amazon Route 53-API-Referenz
- AWS CLI — siehe create-reusable-delegation-setin der AWS CLI Befehlsreferenz
- AWS SDKsDie entsprechende SDK-Dokumentation finden Sie auf der AWS Dokumentationsseite

Schritt 2: Erstellen oder Neuerstellen von gehosteten Amazon Route 53-Zonen und Ändern der TTL für NS- und SOA-Datensätze

Erstellen oder Neuerstellen von Amazon Route 53-gehosteten Zonen:

- Wenn Sie Route 53 derzeit nicht als DNS-Dienst für die Domänen verwenden, für die Sie White-Label-Nameserver verwenden möchten - Erstellen Sie die gehosteten Zonen und geben Sie für jede gehostete Zone die wiederverwendbare Delegierungsgruppe an, die Sie im vorherigen Schritt

erstellt haben. Weitere Informationen finden Sie CreateHostedZonein der Amazon Route 53 API-Referenz.

- Wenn Sie Route 53 derzeit als DNS-Dienst für die Domänen verwenden, für die Sie White-Label-Nameserver verwenden möchten - Erstellen Sie die gehosteten Zonen, für die Sie White-Label-Nameserver verwenden möchten, neu, und geben Sie für jede gehostete Zone die wiederverwendbare Delegierungsgruppe an, die Sie im vorherigen Schritt erstellt haben.

> **Important**
>
> Sie können die Nameserver, die mit einer vorhandenen gehosteten Zone verknüpft sind, nicht mehr ändern. Sie können eine wiederverwendbare Delegierungsgruppe nur dann mit einer gehosteten Zone verknüpfen, wenn Sie die gehostete Zone erstellen.

Beim Erstellen der gehosteten Zonen und bevor Sie auf die Ressourcen für die entsprechenden Domänen zugreifen, ändern Sie die folgenden TTL-Werte für jede gehostete Zone:

- Ändern Sie die TTL für den NS-Datensatz für die gehostete Zone auf 60 Sekunden oder weniger.
- Ändern Sie die Mindest-TTL für den SOA-Datensatz für die gehostete Zone auf 60 Sekunden oder weniger. Dies ist der letzte Wert im SOA-Datensatz.

Wenn Sie Ihrer Vergabestelle versehentlich die falschen IP-Adressen für Ihre White-Label-Nameserver gegeben haben, ist Ihre Website nicht mehr erreichbar und bleibt dies auch für die Dauer der TTL, nachdem Sie das Problem behoben haben. Wenn Sie eine kurze TTL einstellen, ist Ihre Website nur für entsprechend kürzere Zeit nicht verfügbar.

Weitere Informationen zum Erstellen von Hosting-Zonen und zur Angabe eines wiederverwendbaren Delegierungssatzes für die Nameserver für die Hosting-Zonen finden Sie CreateHostedZonein der Amazon Route 53 API-Referenz.

Schritt 3: Erneutes Erstellen von Datensätzen für Ihre gehosteten Zonen

Erstellen Sie Datensätze in den in Schritt 2 erstellten gehosteten Zonen:

- Beim Migrieren des DNS-Dienstes für Ihre Domäne zu Amazon Route 53 können Sie ggf. Datensätze durch Importieren von Informationen über Ihre vorhandenen Datensätze erstellen. Weitere Informationen finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.

- Wenn Sie vorhandene gehostete Zonen austauschen, so dass Sie White Label-Nameserver verwenden können, erstellen Sie in den neuen gehosteten Zonen die Datensätze neu, die in Ihren aktuellen gehosteten Zonen erscheinen. Route 53 bietet keine Methode zum Exportieren von Datensätzen aus einer gehosteten Zone; einige Drittanbietern bieten jedoch diese Möglichkeit. Anschließend können Sie mit dem Route 53-Importfeature Nicht-Alias-Datensätze importieren, für die die Routing-Richtlinie einfach ist. Es gibt keine Möglichkeit, Alias-Datensätze oder Datensätze, für die die Routing-Richtlinie nicht einfach ist, zu exportieren und erneut zu importieren.

  Informationen zum Erstellen von Datensätzen mithilfe der Route 53-API finden Sie CreateHostedZonein der Amazon Route 53-API-Referenz. Informationen zur Erstellung von Datensätzen mit der Route 53-Konsole finden Sie unter Arbeiten mit Datensätzen.

Schritt 4: IP-Adressen abrufen

Rufen Sie die IPv6 Adressen IPv4 und Adressen der Nameserver im wiederverwendbaren Delegierungssatz ab und füllen Sie die folgende Tabelle aus.

Der Name eines Nameservers in Ihrer wiederverwendbaren Delegierungsgruppe (Beispiel: Ns-2048.awsdns-64.com)	IPv4 und IPv6 Adressen	Name, den Sie dem White-Label-Nameserver zuweisen möchten (Beispiel: ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

Angenommen, die vier Nameserver für die wiederverwendbare Delegierungsgruppe sind:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Hier sehen Sie die Linux- und Windows-Befehle, die Sie ausführen müssen, um die IP-Adressen für den ersten Ihrer vier Nameserver abzurufen:

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
```

Schritt 5: Erstellen von Datensätzen für White-Label-Nameserver

Erstellen Sie in der gehosteten Zone mit demselben Namen (z. B. example.com) wie die Domäne des White-Label-Nameservers (z. B. ns1.example.com) acht Datensätze:

- Einen Datensatz A für jeden White-Label-Nameserver
- Einen Datensatz AAAA für jeden White-Label-Nameserver

> **Important**
>
> Wenn Sie dieselben White-Label-Nameserver für zwei oder mehr gehostete Zonen verwenden, führen Sie diesen Schritt nicht für die anderen gehosteten Zonen aus.

Geben Sie für jeden Datensatz die folgenden Werte an. Weitere Informationen finden Sie in der Tabelle, die Sie im vorherigen Schritt ausgefüllt haben:

Routing-Richtlinie

Geben Sie Einfaches Routing an.

Datensatzname

Der Name, den Sie einem Ihrer White-Label-Nameserver zuweisen möchten (Beispiel: ns1.example.com). Für das Präfix (ns1 in diesem Beispiel) können Sie jeden beliebigen Wert verwenden, der in einem Domänennamen gültig ist.

Bewerten/Weiterleiten des Datenverkehrs an

Die IPv4 oder IPv6 Adresse eines der Route 53-Nameserver in Ihrem wiederverwendbaren Delegierungssatz.

> **Important**
>
> Wenn Sie bei der Erstellung von Datensätzen für White-Label-Nameserver falsche IP-Adressen angeben, ist Ihre Website oder Webanwendung im Internet bei der Durchführung von nachfolgenden Schritten nicht mehr verfügbar. Auch wenn Sie die IP-Adressen sofort korrigieren, bleibt Ihre Website oder Webanwendung für die Dauer der TTL unerreichbar.

Datensatztyp

Geben Sie A an, wenn Sie Datensätze für die IPv4 Adressen erstellen.

Geben Sie AAAA an, wenn Sie Datensätze für die IPv6 Adressen erstellen.

TTL (Sekunden)

Dieser Wert ist die Dauer, für die DNS-Resolver die Informationen in diesem Datensatz im Cache speichern, bevor sie eine weitere DNS-Abfrage an Route 53 weiterleiten. Wir empfehlen, dass Sie einen Anfangswert von 60 Sekunden oder weniger festlegen, so dass Sie die Informationen schnell wiederherstellen können, wenn Sie versehentlich falsche Werte in diesen Datensätzen angeben.

Schritt 6: Aktualisieren der NS- und SOA-Datensätze

Aktualisieren Sie SOA- und NS-Datensätze in den gehosteten Zonen, für die Sie White-Label-Nameserver verwenden möchten. Führen Sie Schritt 6 bis Schritt 8 jeweils für eine gehostete Zone und die entsprechende Domäne aus, nicht mehr, und wiederholen Sie anschließend diese Schritte für eine andere gehostete Zone und Domäne.

> **Important**
>
> Beginnen Sie mit der gehosteten Amazon Route 53-Zone mit demselben Domainnamen (z. B. example.com) wie die White-Label-Nameserver (z. B. ns1.example.com).

1. Aktualisieren des SOA-Datensatzes durch Austauschen des Namens des Route 53-Namenservers durch den Namen eines White-Label-Nameservers

   Beispiel

   Ersetzen Sie den Namen des Route 53-Namensservers:

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   durch den Namen eines Ihrer White-Label-Nameserver:

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > Sie haben den letzten Wert, die TTL (Time to Live), unter Schritt 2: Erstellen oder Neuerstellen von gehosteten Amazon Route 53-Zonen und Ändern der TTL für NS- und SOA-Datensätze geändert.

   Informationen zur Aktualisierung von Datensätzen mit der Route 53-Konsole finden Sie unter Bearbeiten von Datensätzen.
2. Notieren Sie sich die Namen der aktuellen Nameserver für die Domäne im NS-Datensatz, sodass Sie diese Nameserver bei Bedarf wiederherstellen können.

3. Aktualisieren Sie den NS-Datensatz. Ersetzen Sie den Namen der Route 53-Nameservers durch die Namen Ihrer vier White-Label-Nameserver, beispielsweise `ns1.example.com`, `ns2.example.com`, `ns3.example.com` und `ns4.example.com`.

Schritt 7: Erstellen und Ändern der Nameserver der Vergabestelle

Verwenden Sie die Methode der Vergabestelle zum Erstellen von Glue-Datensätzen, und ändern Sie die Nameserver der Vergabestelle:

1. Glue-Datensätze hinzufügen:

   - Beim Aktualisieren der Domäne mit demselben Domänennamen wie die White-Label-Nameservee - Erstellen Sie vier Glue-Datensätze, deren Namen und IP-Adressen den Werten entsprechen, die Sie in Schritt 4 abgerufen haben. Nehmen Sie IPv4 sowohl die als auch die IPv6 Adresse für einen White-Label-Nameserver in den entsprechenden Glue-Datensatz auf, zum Beispiel:

     ns1.example.com - IP-Adressen = 192.0.2.117 und 2001:db8:85a3::8a2e:370:7334

     Vergabestellen verwenden unterschiedliche Begriffe für Glue-Datensätze. Dieser Vorgang kann beispielsweise auch als das Registrieren neuer Namenserver oder ähnlich bezeichnet werden.
   - Beim Aktualisieren einer weiteren Domäne – Wenn Route 53 Ihr DNS-Dienst ist, müssen Sie zuerst den Schritt im vorherigen Aufzählungszeichen ausführen und die Glue-Datensätze erstellen, die mit dem Domainnamen übereinstimmen. Anschließend fahren Sie mit Schritt 2 in diesem Verfahren fort.
2. Ändern Sie die Nameserver für die Domäne auf die Namen Ihrer White-Label-Nameserver.

Siehe , wenn sie Amazon Route 53 als DNS-Dienst verwenden, siehe Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Schritt 8: Überwachen des Datenverkehrs für die Website oder Anwendung

Überwachen Sie den Datenverkehr für die Website oder Anwendung, für die Sie in Schritt 7 den Glue-Datensatz erstellt und die Nameserver geändert haben:

- Wenn der Datenverkehr abbricht - Verwenden Sie die Methode der Vergabestelle, um die Nameserver für die Domäne wieder in die vorherigen Route 53-Nameserver zu verwandeln.

Hierbei handelt es sich um die Nameserver, die Sie in Schritt 6b notiert haben. Ergründen Sie anschließend, was schiefgelaufen ist.

- Wenn der Datenverkehr nicht betroffen ist - Wiederholen Sie Schritt 6 bis 8 für die übrigen gehosteten Zonen, für die Sie dieselben White-Label-Nameserver verwenden möchten.

Schritt 9: Kehren Sie zu den ursprünglichen Werten TTLs zurück

Ändern Sie für alle gehosteten Zonen, die nun White-Label-Nameserver verwenden, die folgenden Werte:

- Ändern Sie die TTL für den NS-Datensatz für die gehostete Zone in einen typischen Wert für NS-Datensätze, z. B. 172800 Sekunden (zwei Tage).
- Ändern Sie die Mindest-TTL für den SOA-Datensatz für die gehostete Zone in einen typischen Wert für SOA-Datensätze, z. B. 900 Sekunden. Dies ist der letzte Wert im SOA-Datensatz.

Schritt 10: Kontaktieren von rekursiven DNS-Dienstes (optional)

Optional Wenn Sie Amazon Route 53 Geolocation Routing verwenden, wenden Sie sich an die rekursiven DNS-Dienste, die die edns-client-subnet Erweiterung von EDNS0 unterstützen, und geben Sie ihnen die Namen Ihrer White-Label-Nameserver. Auf diese Weise wird sichergestellt, dass die DNS-Dienste basierend auf der ungefähren Geolokation, von der die Abfrage stammt, weiterhin DNS-Abfragen an den optimalen Route 53-Standort weiterleiten.

NS- und SOA-Datensätze, die Amazon Route 53 für eine öffentliche gehostete Zone erstellt

Bei der Erstellung einer öffentlichen gehosteten Zone erstellt Amazon Route 53 automatisch einen NS-Eintrag (Namenserver) und einen SOA-Eintrag (Start of Authority, Autoritätsursprung) für die Zone. Sie müssen diese Datensätze selten ändern.

Themen

Der Nameserver(NS)-Datensatz

Amazon Route 53 erstellt automatisch einen Namenserver-(NS)-Datensatz mit demselben Namen wie Ihre gehostete Zone. Es listet die vier Nameserver auf, welche die autoritativen Nameserver für Ihre gehostete Zone sind. Außer in seltenen Fällen empfehlen wir, in diesem Datensatz keine Nameserver hinzuzufügen, zu ändern oder zu löschen.

Die folgenden Beispiele zeigen das Format für die Namen von Route 53-Nameservern (diese Beispiele dienen einzig der Veranschaulichung und sind nicht für die Aktualisierung der NS-Datensätze Ihrer Vergabestellt zu verwenden):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

So rufen Sie die Liste der Nameserver für Ihre gehostete Zone ab:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone aus und wählen Sie dann View Details (Details anzeigen) aus.
4. Wählen Sie auf der Detailseite für die gehostete Zone Hosted Zone details (Details der gehosteten Zone) aus.
5. Notieren Sie sich die vier Namen, die für Name Servers (Namenserver) aufgelistet werden.

Weitere Informationen zur Migration des DNS-Dienst von einem anderen DNS-Dienstanbieter zu Route 53 finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Der Start-of-Authority(SOA)-Datensatz

Der State-of-Authority- bzw. SOA-Datensatz identifiziert die Basis-DNS-Informationen über die Domäne, zum Beispiel:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Ein SOA-Datensatz umfasst die folgenden Elemente:

- Der Route 53-Nameserver, der den SOA-Datensatz erstellt hat, z. B. `ns-2048.awsdns-64.net`.
- E-Mail-Adresse des Administrators Das Symbol `@` wird durch einen Punkt ersetzt, z. B. `hostmaster.example.com`. Der Standardwert ist ein amazon.com-E-Mail-Adresse, die nicht überwacht wird.
- Eine Seriennummer, die Sie optional erhöhen können, wenn Sie einen Datensatz in der gehosteten Zone aktualisieren. erhöht den Wert nicht automatisch. Route 53 erhöht die Zahl nicht automatisch. (Die Seriennummer wird von DNS-Dienstes verwendet, die sekundäre DNS unterstützen.) In dem Beispiel lautet dieser Wert `1`.
- Eine Aktualisierungszeit in Sekunden, die sekundäre DNS-Server warten, bevor sie den SOA-Datensatz des primären DNS-Servers abrufen, um auf Änderungen zu prüfen. In dem Beispiel lautet dieser Wert `7200`.
- Das Intervall in Sekunden, das ein sekundärer Server bis zur Wiederholung einer fehlgeschlagenen Zonenübertragung abwartet. Normalerweise ist die Zeit bis zu einem Neuversuch kürzer als bis zu einer Aktualisierung. In dem Beispiel lautet dieser Wert `900` (15 Minuten).
- Die Zeit in Sekunden, für die ein sekundärer Server versucht, eine Zonenübertragung abzuschließen. Wenn diese Zeit abgelaufen ist, bevor eine Zonenübertragung erfolgreich abgeschlossen werden konnte, beantwortet der sekundäre Server keine Abfragen mehr, da er seine Daten als zu alt einstuft, um noch zuverlässig zu sein. In dem Beispiel lautet dieser Wert `1209600` (zwei Wochen).
- Die Mindest-TTL (Time-to-live). Dieser Wert hilft, die Zeitspanne zu definieren, aus der rekursive Resolver die folgenden Antworten von Route 53 zwischenspeichern sollten:

  NXDOMAIN

  Es gibt keinen Datensatz eines Typs mit dem Namen, der in der DNS-Abfrage angegeben ist, z. B. example.com. Es gibt auch keine Datensätze, die untergeordnete Elemente des Namens sind, der in der DNS-Abfrage angegeben ist, z. B. zenith.example.com.

  NODATA

  Es gibt mindestens einen Datensatz mit dem Namen, der in der DNS-Abfrage angegeben ist, aber keiner dieser Datensätze hat den Typ (z. B. A), der in der DNS-Abfrage angegeben ist.

  Wenn ein DNS-Resolver eine NXDOMAIN oder NODATA-Antwort zwischenspeichert, wird dies als Negative Cachingbezeichnet.

Die Dauer des Negative Caching ist kürzer als die folgenden Werte:

- Dieser Wert — die Mindest-TTL im SOA-Datensatz. In dem Beispiel lautet der Wert `86400` (ein Tag).
- Der TTL-Wert für den SOA-Datensatz. Der Standardwert beträgt 900 Sekunden. Weitere Informationen zum Ändern dieses Werts finden Sie unter Bearbeiten von Datensätzen.

Wenn Route 53 auf DNS-Abfragen mit einer NXDOMAIN- oder NODATA-Antwort antwortet (eine negative Antwort), wird Ihnen die Rate für Standardabfragen berechnet. (Siehe „Abfragen“ in Amazon Route 53. Wenn Sie Bedenken hinsichtlich der Kosten für negative Antworten haben, können Sie die TTL für den SOA-Datensatz, die minimale TTL im SOA-Datensatz (dieser Wert) oder beides ändern. Beachten Sie, dass eine Erhöhung dieser Werte TTLs, die sich auf negative Antworten für die gesamte Hosting-Zone beziehen, sowohl positive als auch negative Auswirkungen haben kann:

- DNS-Resolver im Internet zwischenspeichern das Nichtvorhandensein von Datensätzen für längere Zeiträume, wodurch die Anzahl der Abfragen reduziert wird, die an Route 53 weitergeleitet werden. Dies reduziert die Route 53-Kosten für DNS-Abfragen.
- Wenn Sie jedoch einen gültigen Datensatz fälschlicherweise löschen und ihn später neu erstellen, speichern DNS-Resolver die negative Antwort (dieser Datensatz existiert nicht) für einen längeren Zeitraum. Dadurch wird die Zeit verlängert, für die Ihre Kunden oder Benutzer die entsprechende Ressource nicht erreichen können, z. B. einen Webserver für acme.example.com.

So finden Sie Ihre SOA-Datensätze in Route 53

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den verknüpften Namen der Domäne aus, für die Sie Datensätze anzeigen möchten.
4. Im Abschnitt Records (Datensätze) können Sie alle aufgelisteten Datensätze anzeigen und die Datensätze auch filtern, um Ihren SOA-Wert zu finden.

Aktivierung der beschleunigten Wiederherstellung für die Verwaltung öffentlicher DNS-Einträge

Route 53 Accelerated Recovery für die Verwaltung öffentlicher DNS-Einträge ist so konzipiert, dass ein 60-minütiges Recovery Time Objective (RTO) erreicht wird, falls der Dienst in der Region USA Ost (Nord-Virginia) nicht verfügbar ist. Wenn die Option für eine öffentlich gehostete Route 53-Zone aktiviert ist, können Sie innerhalb von etwa 60 Minuten wieder Änderungen an DNS-Einträgen in der öffentlich gehosteten Zone vornehmen, nachdem AWS festgestellt wurde, dass der Betrieb in der Region USA Ost (Nord-Virginia) beeinträchtigt ist.

Important

Die beschleunigte Wiederherstellung ist nur für öffentlich gehostete Zonen verfügbar. Private gehostete Zonen werden nicht unterstützt.

Note

Die DNS-Abfrageauflösung auf der Route 53-Datenebene funktioniert auch bei Störungen des regionalen Dienstes normal. Unter Resilienz in Route 53 finden Sie Informationen zu den Vorgängen auf Datenebene und auf Kontrollebene.

Themen

So funktioniert die beschleunigte Wiederherstellung von öffentlichen DNS-Einträgen

Wenn die beschleunigte Wiederherstellung aktiviert ist, verwaltet Route 53 eine Kopie Ihrer öffentlich gehosteten Zone in der Region USA West (Oregon). Wenn Dienste in der Region USA Ost (Nord-

Virginia) für einen längeren Zeitraum nicht verfügbar sind, führt Route 53 innerhalb von 60 Minuten einen Failover durch und leitet den Betrieb der Steuerungsebene für Ihre öffentlich gehosteten Zonen mit aktivierter beschleunigter Wiederherstellung automatisch in die Region USA West (Oregon) um. Sie können dann weiterhin programmgesteuert DNS-Änderungen über die CLI, das SDK und die API vornehmen. Beachten Sie, dass während des Failovers eine begrenzte Anzahl von API-Methoden verfügbar sein wird. Weitere Informationen finden Sie im Abschnitt „Zusätzliche Überlegungen“. Wenn sich die Region erholt, führt Route 53 das Failback-Verfahren durch und leitet den Betrieb der Kontrollebene automatisch zurück in die Region USA Ost (Nord-Virginia).

> **Note**
>
> Bevor die Region USA Ost (Nord-Virginia) beeinträchtigt wird, müssen Sie zunächst die beschleunigte Wiederherstellung für die Verwaltung öffentlicher DNS-Einträge in Ihrer öffentlich gehosteten Zone aktivieren. Dies kann über die Konsole, die CLI, das SDK oder die API erfolgen (siehe den Abschnitt So aktivieren Sie die beschleunigte Wiederherstellung für die Verwaltung öffentlicher DNS-Einträge auf dieser Seite unten). Sie können die beschleunigte Wiederherstellung nicht für die Verwaltung öffentlicher DNS-Einträge nach einem Failover aktivieren.

Erneutes Senden von DNS-Änderungen nach einem Failover

Unter normalen Bedingungen werden Änderungen an öffentlich gehosteten Zonen mit aktivierter beschleunigter Wiederherstellung von der Region USA Ost (Nord-Virginia) akzeptiert und anschließend erfolgreich in die Region USA West (Oregon) repliziert. Wenn es jedoch in der Region USA Ost (Nord-Virginia) zu einer Betriebsunterbrechung kommt, werden einige Änderungen möglicherweise von der Region USA Ost (Nord-Virginia) akzeptiert, aber möglicherweise nicht in die Region USA West (Oregon) repliziert. Diese Änderungen während des Fluges werden als „gestrandete Änderungen“ bezeichnet. Sobald das Failover abgeschlossen ist, empfiehlt Route 53, dass Sie ungenutzte Änderungen erneut einreichen, bevor Sie Ihre DNS-Workflows wieder aufnehmen. Sie können dies entweder mithilfe der API oder mithilfe AWS CloudFormation der unten beschriebenen Methoden erreichen.

Verwenden der API zum Verfolgen und Einreichen von DNS-Änderungen

Wenn Sie die Route 53-API, AWS CLI oder AWS SDKs zur Verwaltung von DNS-Einträgen verwenden, müssen Sie die ChangeResourceRecordSets API und die GetChange API verwenden, um DNS-Änderungen einzureichen bzw. zu verfolgen.

Wenn Sie die ChangeResourceRecordSets API verwenden, um DNS-Änderungen vorzunehmen, gibt Route 53 eine Kennung (ID) für die von Ihnen vorgenommene Änderung zurück (Einzelheiten ChangeInfozum Objekt der Änderungsantwort finden Sie unter). Sie können diese ID in einer nachfolgenden Anfrage an die GetChange API angeben und den Status der Änderung beobachten. DNS-Änderungen mit dem Status INSYNC wurden in die Region USA West (Oregon) repliziert und an alle Route 53-DNS-Server weitergegeben. Vor oder nach einem Failover müssen Sie keine weiteren Maßnahmen ergreifen, um diese Änderungen zu berücksichtigen. Während einer Beeinträchtigung der Region USA Ost (Nord-Virginia) kann es jedoch GetChange sein, dass der Status PENDING zurückgegeben wird, was darauf hindeutet, dass Ihre Änderung möglicherweise nicht in die Region USA West (Oregon) repliziert wurde. Wenn das der Fall ist, kehrt der Failover nach Abschluss des Failovers zurück, GetChange was darauf hinweist NoSuchChange, dass Route 53 diese DNS-Änderung nicht replizieren konnte. Daher können Sie nach einem Failover diese fehlgeschlagenen DNS-Änderungen getrost ignorieren und sie als neue DNS-Änderungen erneut einreichen. Sie werden wissen, dass der Failover-Prozess abgeschlossen ist, wenn Route 53 eine Nachricht an das AWS Health Dashboard sendet.

Wird verwendet AWS CloudFormation , um Änderungen nachzuverfolgen und einzureichen

AWS CloudFormation verfolgt mithilfe der GetChange API automatisch den Replikationsstatus Ihrer DNS-Änderungen und schließt ein Update erst ab, wenn die DNS-Änderungen als INSYNC bestätigt wurden. Wenn Sie DNS-Einträge CloudFormation zur Verwaltung verwenden und die Region USA Ost (Nord-Virginia) nicht mehr verfügbar ist, können die Aktionen, die Sie verwenden, während des Zeitraums der Nichtverfügbarkeit nicht erfolgreich abgeschlossen CloudFormation werden. Sie können jedoch einfach dieselben Aktionen wiederholen, um DNS-Änderungen erneut einreichen CloudFormation zu können, sobald der Route 53-Failover-Prozess abgeschlossen ist.

Failback zur Region USA Ost (Nord-Virginia)

Route 53 führt ein Failback für den Betrieb der Kontrollebene für Ihre öffentlich gehostete Zone auf die Region USA Ost (Nord-Virginia) durch, sobald sich die Region erholt hat. Während des Failbacks müssen Sie Ihre DNS-Änderungen nicht erneut einreichen, da bei diesem Vorgang keine Änderungen vorgenommen werden, die in der Vergangenheit gespeichert wurden.

Weitere Überlegungen

Im Zusammenhang mit der Funktion zur beschleunigten Wiederherstellung sollten Sie einige zusätzliche Überlegungen beachten:

1. Sie können während eines Failovers keine neuen Hosting-Zonen erstellen, bestehende Hosting-Zonen löschen, die DNSSEC-Signatur aktivieren oder die DNSSEC-Signatur deaktivieren.

2. AWS PrivateLink Verbindungen funktionieren nach einem Failover nicht, funktionieren aber nach einem Failback in die Region USA Ost (Nord-Virginia) wieder.
3. CloudFront Pauschalpläne werden derzeit nicht unterstützt.
4. Gehostete Zonen mit aktivierter beschleunigter Wiederherstellung können nicht gelöscht werden. Sie müssen die beschleunigte Wiederherstellung deaktivieren, bevor Sie versuchen, die gehostete Zone zu löschen.
5. Während eines Failovers werden die folgenden API-Methoden für öffentlich gehostete Zonen mit aktivierter beschleunigter Wiederherstellung weiterhin unterstützt. Alle anderen Route 53-API-Methoden funktionieren jedoch erst, wenn ein Failback auftritt.
   - `ChangeResourceRecordSets`
   - `GetChange`
   - `GetGeoLocation`
   - `GetHostedZone`
   - `GetHostedZoneCount`
   - `GetHostedZoneLimit`
   - `GetReusableDelegationSet`
   - `GetReusableDelegationSetLimit`
   - `ListGeoLocations`
   - `ListHostedZones`
   - `ListHostedZonesByName`
   - `ListResourceRecordSets`
   - `ListReusableDelegationSets`

Wie aktiviert man eine beschleunigte Wiederherstellung für die Verwaltung öffentlicher DNS-Einträge

Sie können die beschleunigte Wiederherstellung für die Verwaltung öffentlicher DNS-Einträge mithilfe der Route 53-Konsole, API, CLI oder SDK aktivieren. Die Zeit, die benötigt wird, um die beschleunigte Wiederherstellung zu aktivieren, hängt von der Größe Ihrer öffentlich gehosteten Zone und anderen Faktoren ab. Sie sollten einplanen, dass der Vorgang zur Aktivierung der beschleunigten Wiederherstellung mehrere Stunden in Anspruch nimmt. Sie können den Status des Aktivierungsprozesses auf der Registerkarte Beschleunigte Wiederherstellung in Ihrer öffentlich gehosteten Zone oder über die `GetHostedZone` API überprüfen. Nach Abschluss des Vorgangs wird es einen kurzen Zeitraum von bis zu mehreren Minuten geben, in dem DNS-Änderungen nicht

akzeptiert werden. Sobald die DNS-Änderungen abgeschlossen sind, können sie wie gewohnt fortgesetzt werden.

Um die beschleunigte Wiederherstellung mit der Route 53-Konsole zu aktivieren und zu deaktivieren

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie die öffentlich gehostete Zone aus, für die Sie die beschleunigte Wiederherstellung aktivieren möchten.
4. Wählen Sie auf der Registerkarte Beschleunigte Wiederherstellung die Option Aktivieren aus.
5. Wählen Sie Änderungen speichern aus.
6. Überwachen Sie den Status der gehosteten Zone. Der Status zeigt während der Installation Enabling Accelerated Recovery an und wechselt nach Abschluss zu Aktiviert.

Sie können die beschleunigte Wiederherstellung mit den gleichen Schritten wie oben deaktivieren, aber stattdessen Deaktivieren wählen.

CLI-Beispiel zum Aktivieren

```
aws route53 update-hosted-zone-features --enable-accelerated-recovery --hosted-zone-id
 Z123456789
```

CLI-Beispiel zum Deaktivieren

```
aws route53 update-hosted-zone-features --no-enable-accelerated-recovery --hosted-zone-
id Z123456789
```

Arbeiten mit privat gehosteten Zonen

Eine private gehostete Zone ist ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer Domains antworten soll VPCs , die Sie mit dem Amazon VPC-Service erstellen. Privat gehostete Zonen funktionieren folgendermaßen:

1. Sie erstellen Sie eine privat gehostete Zone, z. B. example.com, und geben die VPC an, die Sie der gehosteten Zone zuordnen möchten. Nachdem Sie die gehostete Zone erstellt haben, können Sie ihr weitere VPCs zuordnen.

2. Sie erstellen Datensätze in der Hosting-Zone, die festlegen, wie Route 53 auf DNS-Anfragen für Ihre Domain und Subdomains innerhalb und zwischen Ihren VPCs reagiert. Nehmen wir beispielsweise an, Sie haben einen Datenbankserver, der auf einer EC2 Instance in der VPC läuft, die Sie Ihrer privaten Hosting-Zone zugeordnet haben. Sie erstellen einen A- oder AAAA-Datensatz, wie z. B. db.example.com, und geben die IP-Adresse des Datenbankservers an.

   Weitere Informationen über Einträge finden Sie unter Arbeiten mit Datensätzen. Weitere Informationen über die Amazon-VPC-Anforderungen für die Verwendung von privat gehosteten Zonen finden Sie unter Verwenden von privat gehosteten Zonen im Amazon-VPC-Benutzerhandbuch.
3. Wenn eine Anwendung eine DNS-Abfrage für db.example.com sendet, gibt Route 53 die entsprechende IP-Adresse zurück. Um eine Antwort von einer privaten gehosteten Zone zu erhalten, müssen Sie außerdem eine EC2 Instanz in einer der zugehörigen Zonen ausführen VPCs (oder über einen eingehenden Endpunkt aus einem Hybrid-Setup verfügen). Wenn Sie versuchen, eine private gehostete Zone von außerhalb des VPCs oder Ihres Hybrid-Setups abzufragen, wird die Anfrage rekursiv im Internet gelöst.
4. Die Anwendung verwendet die IP-Adresse, die sie von Route 53 erhalten hat, um eine Verbindung mit dem Datenbankserver herzustellen.

Wenn Sie eine privat gehostete Zone erstellen, werden die folgenden Nameserver verwendet:

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

Diese Nameserver werden verwendet, weil das DNS-Protokoll verlangt, dass für jede gehostete Zone ein Nameserver-Datensatz festgelegt werden muss. Diese Nameserver sind reserviert und werden nie von öffentlich gehosteten Route-53-Zonen verwendet. Sie können diese Zonen nur über VPC Resolver in einer VPC abfragen, die der gehosteten Zone zugeordnet wurde, indem Sie einen eingehenden Endpunkt verwenden, der mit der in der privaten gehosteten Zone VPCs angegebenen Verbindung verbunden ist.

Während die Nameserver im Internet sichtbar sind, stellt VPC Resolver keine Verbindung zu den Nameserveradressen her. Außerdem werden die Informationen zur privaten gehosteten Zone nicht zurückgegeben, wenn Sie die Nameserver direkt über das Internet abfragen. Stattdessen

erkennt der VPC-Resolver, dass sich Abfragen innerhalb eines privaten Namespaces befinden, der auf Verbindungen zwischen VPC und gehosteten Zonen basiert, und verwendet direkte, private Konnektivität, um die privaten DNS-Server zu erreichen.

> **Note**
>
> Sie können den Nameserver-Datensatz in einer privaten gehosteten Zone ändern, wenn Sie möchten, und die private DNS-Auflösung wird weiterhin funktionieren. Wir raten davon ab, aber wenn Sie sich dafür entscheiden, sollten Sie reservierte Domänennamen verwenden, die nicht von öffentlichen DNS-Servern verwendet werden.

Wenn Sie Datenverkehr an Ihre Domäne im Internet weiterleiten wollen, können Sie eine öffentliche von Route 53 gehostete Zone verwenden. Weitere Informationen finden Sie unter Arbeiten mit öffentlichen gehosteten Zonen.

Themen

Überlegungen zum Arbeiten mit einer privaten gehosteten Zone

Beachten Sie die folgenden Überlegungen zur Verwendung von privaten gehosteten Zonen.

- Amazon VPC settings
- Route 53 health checks
- Supported routing policies for records in a private hosted zone
- Split-view DNS

- Public and private hosted zones that have overlapping namespaces
- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 VPC Resolver rules
- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Amazon VPC-Einstellungen

Zur Verwendung von privat gehosteten Zonen müssen Sie die folgenden Amazon-VPC-Einstellungen auf `true` setzen:

- `enableDnsHostnames`
- `enableDnsSupport`

Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC anzeigen und aktualisieren im Amazon VPC-Benutzerhandbuch.

Route 53 Zustandsprüfungen

In einer privat gehosteten Zone können Sie Route 53-Zustandsprüfungen nur mit Failover-, mehrwertigen Antworten-, Gewichtungs-, Latenz-, Geolokalisierungs- und Geoproximitätsdatensätzen verknüpfen. Weitere Informationen zum Zuordnen von Zustandsprüfungen zu Failover-Datensätzen finden Sie unter Konfigurieren von Failover in einer privaten gehosteten Zone.

Unterstützte Routing-Richtlinien für Datensätze in einer privaten gehosteten Zone

Sie können die folgenden Routing-Richtlinien verwenden, wenn Sie Datensätze in einer privat gehosteten Zone erstellen:

- Einfaches Routing
- Failover-Routing
- Mehrwertiges Antwort-Routing
- Gewichtetes Routing
- Latenzbasiertes Routing
- Geolocation-Routing
- Geoproximity-Routing

Sie können keine Datensätze in einer privat gehosteten Zone mit anderen Routing-Richtlinien erstellen.

Split-View-DNS

Sie können Route 53 verwenden, um Split-View-DNS (auch als Split-Horizon-DNS bekannt) zu konfigurieren. In Split-View-DNS verwenden Sie denselben Domänennamen (example.com) für interne Zwecke (accounting.example.com) und externe Zwecke, z. B. für Ihre öffentliche Website (www.example.com). Sie können auch denselben Subdomänennamen intern und extern verwenden, aber unterschiedliche Inhalte bereitstellen oder eine unterschiedliche Authentifizierung für interne und externe Benutzer erfordern.

Um Split-View-DNS zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Erstellen Sie öffentliche und private gehostete Zonen mit demselben Namen. (Split-View-DNS funktioniert auch weiterhin, wenn Sie einen anderen DNS-Service für die öffentliche gehostete Zone verwenden.)
2. Ordnen Sie der privaten VPCs Hosting-Zone ein oder mehrere Amazon zu. Route 53 VPC Resolver verwendet die private gehostete Zone, um DNS-Abfragen in der angegebenen Zone weiterzuleiten. VPCs
3. Erstellen Sie Datensätze in jeder gehosteten Zone. Aufzeichnungen in der öffentlich gehosteten Zone steuern, wie der Internetverkehr weitergeleitet wird, und Aufzeichnungen in der privaten gehosteten Zone steuern, wie der Verkehr in Ihrem Amazon weitergeleitet wird. VPCs

Wenn Sie die Namensauflösung sowohl für Ihre VPC- als auch für Ihre lokalen Workloads durchführen müssen, können Sie Route 53 VPC Resolver verwenden. Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.

Öffentliche und private gehostete Zonen mit überlappenden Namespaces

Wenn Sie private und öffentliche Hosting-Zonen mit sich überschneidenden Namespaces haben, z. B. example.com und accounting.example.com, leitet VPC Resolver den Verkehr auf der Grundlage der genauesten Übereinstimmung weiter. Wenn Benutzer bei einer EC2 Instance in einer Amazon VPC angemeldet sind, die Sie der privaten Hosting-Zone zugeordnet haben, verarbeitet Route 53 VPC Resolver DNS-Abfragen wie folgt:

1. VPC Resolver bewertet, ob der Name der privaten gehosteten Zone mit dem Domainnamen in der Anfrage übereinstimmt, z. B. accounting.example.com. Eine Übereinstimmung wird wie folgt definiert (entweder/oder):
   - Eine identische Übereinstimmung

- Der Name der privat gehosteten Zone ist ein übergeordneter Domänenname in der Anforderung. Angenommen, der Domänenname in der Anforderung lautet wie folgt:

  seattle.finanzen.beispiel.com

  Die folgenden gehosteten Zonen stimmen überein, da sie "seattle.finanzen.beispiel.com" übergeordnet sind:

  - finanzen.beispiel.com
  - example.com

Wenn es keine passende private gehostete Zone gibt, leitet VPC Resolver die Anfrage an einen öffentlichen DNS-Resolver weiter, und Ihre Anfrage wird als reguläre DNS-Anfrage gelöst.

2. Wenn es eine privat gehostete Zone gibt, die dem Domänennamen in der Anforderung entspricht, wird die gehostete Zone nach einem Datensatz durchsucht, der dem Domänennamen und dem DNS-Datensatz in der Anforderung entspricht, z. B. ein A-Datensatz für „accounting.example.com“.

> **Note**
>
> Wenn es eine passende private gehostete Zone gibt, aber kein Datensatz vorhanden ist, der dem Domainnamen und dem Typ der Anfrage entspricht, leitet VPC Resolver die Anfrage nicht an einen öffentlichen DNS-Resolver weiter. Stattdessen wird NXDOMAIN (nicht existierende Domäne) an den Client zurückgegeben.

Öffentliche und private gehostete Zonen mit überlappenden Namespaces

Wenn Sie über zwei oder mehr privat gehostete Zonen mit überlappenden Namespaces verfügen, z. B. example.com und accounting.example.com, leitet VPC Resolver den Verkehr auf der Grundlage der genauesten Übereinstimmung weiter.

> **Note**
>
> Wenn Sie über eine private gehostete Zone (example.com) und eine Route 53 53-VPC-Resolver-Regel verfügen, die den Datenverkehr für denselben Domainnamen an Ihr Netzwerk weiterleitet, hat die VPC-Resolver-Regel Vorrang. Siehe Private hosted zones and Route 53 VPC Resolver rules.

Wenn Benutzer bei einer EC2 Instance in einer Amazon VPC angemeldet sind, die Sie mit allen privaten Hosting-Zonen verknüpft haben, behandelt VPC Resolver DNS-Abfragen wie folgt:

1. VPC Resolver bewertet, ob der Domainname in der Anfrage, z. B. accounting.example.com, mit dem Namen einer der privaten gehosteten Zonen übereinstimmt.
2. Wenn es keine gehostete Zone gibt, die genau mit dem Domainnamen in der Anfrage übereinstimmt, sucht VPC Resolver nach einer gehosteten Zone, deren Name dem Domainnamen in der Anfrage übergeordnet ist. Angenommen, der Domänenname in der Anforderung lautet wie folgt:

   `seattle.accounting.example.com`

   Die folgenden gehosteten Zonen stimmen überein, weil sie übergeordnete Zonen von `seattle.accounting.example.com` sind:

   - `accounting.example.com`
   - `example.com`

   VPC Resolver wählt`accounting.example.com`, weil es spezifischer ist als. `example.com`
3. VPC Resolver durchsucht die `accounting.example.com` gehostete Zone nach einem Datensatz, der dem Domainnamen und dem DNS-Typ in der Anfrage entspricht, z. B. einem A-Eintrag für. `seattle.accounting.example.com`

   Wenn es keinen Datensatz gibt, der dem Domainnamen und dem Typ der Anfrage entspricht, gibt VPC Resolver NXDOMAIN (nicht existierende Domäne) an den Client zurück.

Private gehostete Zonen und Route 53 VPC Resolver-Regeln

Wenn Sie über eine private gehostete Zone (example.com) und eine VPC-Resolver-Regel verfügen, die den Datenverkehr für denselben Domainnamen an Ihr Netzwerk weiterleitet, hat die VPC-Resolver-Regel Vorrang.

Angenommen, folgende Konfiguration liegt vor:

- Sie haben eine private gehostete Zone namens example.com und verknüpfen sie mit einer VPC.
- Sie erstellen eine Route 53 VPC Resolver-Regel, die den Datenverkehr für example.com an Ihr Netzwerk weiterleitet, und ordnen die Regel derselben VPC zu.

In dieser Konfiguration hat die VPC-Resolver-Regel Vorrang vor der privaten Hosting-Zone. DNS-Abfragen werden an Ihr Netzwerk weitergeleitet, anstatt basierend auf den Datensätzen in der privaten gehosteten Zone aufgelöst zu werden.

Delegieren der Verantwortlichkeit für eine Subdomäne

Sie können jetzt NS-Einträge in einer privaten Hosting-Zone erstellen, um die Verantwortung für eine Subdomain zu delegieren. Weitere Informationen finden Sie unter Tutorial zu Resolver-Delegierungsregeln.

Benutzerdefinierte DNS-Server

Wenn Sie benutzerdefinierte DNS-Server auf EC2 Amazon-Instances in Ihrer VPC konfiguriert haben, müssen Sie diese DNS-Server so konfigurieren, dass Ihre privaten DNS-Abfragen an die IP-Adresse der von Amazon bereitgestellten DNS-Server für Ihre VPC weitergeleitet werden. Diese IP-Adresse ist die IP-Adresse an der Basis der VPC-Netzwerkbereichs "plus zwei". Wenn beispielsweise den CIDR-Bereich für Ihre VPC 10.0.0.0/16 lautet, ist die IP-Adresse des DNS-Servers 10.0.0.2.

Wenn Sie DNS-Abfragen zwischen VPCs und Ihrem Netzwerk weiterleiten möchten, können Sie VPC Resolver verwenden. Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.

Erforderliche IAM-Berechtigungen

Um privat gehostete Zonen zu erstellen, müssen Sie zusätzlich zu den Berechtigungen für Route EC2 53-Aktionen auch IAM-Berechtigungen für Amazon-Aktionen gewähren. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53 in der Service-Autorisierungs-Referenz.

Erstellen einer privat gehosteten Zone

Eine privat gehostete Zone ist ein Container für Datensätze für eine Domain, die Sie in einer oder mehreren Amazon Virtual Private Clouds (VPCs) hosten. Sie erstellen eine Hosting-Zone für eine Domain (z. B. example.com) und erstellen dann Datensätze, um Amazon Route 53 mitzuteilen, wie der Traffic für diese Domain innerhalb und zwischen Ihren weitergeleitet werden soll. VPCs

Important

Wenn Sie eine privat gehostete Zone erstellen, müssen Sie eine VPC mit der gehosteten Zone verknüpfen, und die angegebene VPC muss mit demselben Konto erstellt worden sein, indem Sie die gehostete Zone erstellt haben. Nachdem Sie die Hosting-Zone erstellt haben, können Sie ihr weitere zuordnen, einschließlich der Zone, VPCs die Sie VPCs mit einem anderen AWS Konto erstellt haben.

Um VPCs das, was Sie mit einem Konto erstellt haben, einer privaten gehosteten Zone zuzuordnen, die Sie mit einem anderen Konto erstellt haben, müssen Sie die Zuordnung autorisieren und dann die Zuordnung programmgesteuert vornehmen. Weitere Informationen finden Sie unter Zuordnen einer Amazon VPC und einer privaten gehosteten Zone, die Sie mit verschiedenen Konten erstellt haben AWS.

Informationen zur Verwendung von privat gehosteten Zonen durch die Route 53-API finden Sie unter Amazon-Route 53-API-Referenz.

So erstellen Sie eine privat gehostete Zone mit der Route 53-Konsole

1. Für jede VPC, die Sie der gehosteten Route 53-Zone zuordnen möchten, ändern Sie die folgenden VPC-Einstellungen in `true`:

   - `enableDnsHostnames`
   - `enableDnsSupport`

   Weitere Informationen finden Sie unter Anzeigen und Aktualisieren der DNS-Unterstützung für Ihre VPC im Amazon-VPC-Benutzerhandbuch.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
3. Wenn Sie noch keine Erfahrung mit Route 53 haben, wählen Sie Get Started (Erste Schritte) aus.

   Wenn Sie Route 53 bereits nutzen, wählen Sie Hosted zones im Navigationsbereich aus.
4. Wählen Sie Create Hosted Zone (Gehostete Zone erstellen).
5. Geben Sie im Bereich Create Private Hosted Zone (Privat gehostete Zone erstellen) einen Domänennamen und optional einen Kommentar ein.

   Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.
6. Wählen Sie in der Liste Type (Typ) die Option Private Hosted Zone for (Privat gehostete Zone für VPC) aus.
7. Wählen Sie in der Liste VPC ID die VPC aus, die Sie der gehosteten Zone zuordnen möchten.

> **Note**
>
> Wenn die Konsole die folgende Meldung anzeigt: Sie versuchen eine gehostete Zone zu verknüpfen, die denselben Namespace wie der einer anderen gehosteten Zone innerhalb derselben VPC verwendet:
> "Eine in Konflikt stehende Domäne wurde bereits dieser VPC oder dem Delegierungssatz zugeordnet."
> Wenn beispielsweise die gehostete Zone A und die gehostete Zone B denselben Domänennamen, beispielsweise `example.com`, haben, können Sie nicht beide gehosteten Zonen derselben VPC zuordnen.

8. Wählen Sie Create Hosted Zone (Gehostete Zone erstellen).

Auflisten der privaten gehosteten Zonen

Sie können die Amazon Route 53-Konsole verwenden, um alle Hosting-Zonen aufzulisten, die Sie mit dem aktuellen AWS Konto erstellt haben. Informationen zum Auflisten von Hosting-Zonen mithilfe der Route 53-API finden Sie ListHostedZonesin der Amazon Route 53-API-Referenz.

Um die Hosting-Zonen aufzulisten, die einem AWS Konto zugeordnet sind

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

   Auf der Seite „Gehostete Zonen“ wird automatisch eine Liste aller Hosting-Zonen angezeigt, die mit dem aktuellen AWS Konto erstellt wurden. Die Spalte Type gibt an, ob eine gehostete Zone privat oder öffentlich ist. Wählen Sie die Spaltenüberschrift aus, um alle privat gehosteten Zonen und alle öffentlich gehosteten Zonen zu gruppieren.

Einer privaten VPCs Hosting-Zone mehr zuordnen

Sie können die Amazon Route 53-Konsole verwenden, um mehr VPCs mit einer privaten gehosteten Zone zu verknüpfen, wenn Sie die gehostete Zone erstellt haben und dann dasselbe AWS Konto verwenden. VPCs

> **Important**
>
> Wenn Sie VPCs das, was Sie mit einem Konto erstellt haben, einer privaten gehosteten Zone zuordnen möchten, die Sie mit einem anderen Konto erstellt haben, müssen Sie die Zuordnung zuerst autorisieren. Darüber hinaus können Sie die AWS Konsole weder verwenden, um die Zuordnung zu autorisieren noch sie VPCs mit der Hosting-Zone zu verknüpfen. Weitere Informationen finden Sie unter Zuordnen einer Amazon VPC und einer privaten gehosteten Zone, die Sie mit verschiedenen Konten erstellt haben AWS.

Informationen darüber, wie Sie mithilfe der Route 53-API mehr VPCs mit einer privaten gehosteten Zone verknüpfen können, finden Sie unter Associate VPCWith HostedZone in der Amazon Route 53-API-Referenz.

Um mithilfe der Route 53-Konsole zusätzliche VPCs Verbindungen zu einer privat gehosteten Zone herzustellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie das Optionsfeld für die private gehostete Zone aus, der Sie mehr VPCs zuordnen möchten.
4. Wählen Sie Bearbeiten aus.
5. Klicken Sie auf Add VPC (VPC hinzufügen).
6. Wählen Sie die Region aus, in der Sie die VPC erstellt haben, die Sie dieser gehosteten Zone zuordnen möchten.
7. Um dieser VPCs Hosting-Zone mehr zuzuordnen, wiederholen Sie die Schritte 5 und 6.
8. Wählen Sie Änderungen speichern aus.

Zuordnen einer Amazon VPC und einer privaten gehosteten Zone, die Sie mit verschiedenen Konten erstellt haben AWS

Wenn Sie eine VPC, die Sie mit einem AWS Konto erstellt haben, einer privaten gehosteten Zone zuordnen möchten, die Sie mit einem anderen Konto erstellt haben, gehen Sie wie folgt vor:

Um eine Amazon-VPC und eine private gehostete Zone, die Sie erstellt haben, mit verschiedenen AWS Konten zu verknüpfen

1. Autorisieren Sie mit dem Konto, das die gehostete Zone erstellt hat, die Verknüpfung der VPC mit der privat gehosteten Zone mithilfe einer der folgenden Methoden:

   - AWS CLI— Siehe create-vpc-association-authorizationin der AWS CLI Befehlsreferenz
   - AWS SDK oder AWS Tools for Windows PowerShell— Die entsprechende Dokumentation finden Sie auf der AWS Dokumentationsseite
   - Amazon Route 53-API — siehe VPCAssociationAutorisierung erstellen in der Amazon Route 53-API-Referenz

   Beachten Sie Folgendes:

   - Wenn Sie mehrere VPCs , die Sie mit einem Konto erstellt haben, einer gehosteten Zone zuordnen möchten, die Sie mit einem anderen Konto erstellt haben, müssen Sie für jede VPC eine Autorisierungsanfrage einreichen.
   - Wenn Sie die Verknüpfung autorisieren, müssen Sie die gehostete Zonen-ID angeben, daher muss die privat gehostete Zone bereits vorhanden sein.
   - Sie können die Route 53-Konsole nicht verwenden, um die Verknüpfung einer VPC mit einer privat gehosteten Zone zu autorisieren oder um die Verknüpfung durchzuführen.
2. Verwenden Sie das Konto, mit dem Sie die VPC erstellt haben, um die VPC mit der gehosteten Zone zu verknüpfen. Wie bei der Autorisierung der Zuordnung können Sie das AWS SDK, Tools for Windows PowerShell AWS CLI, die oder die Route 53-API verwenden. Wenn Sie die API verwenden, verwenden Sie die VPCWith HostedZone Aktion Zuordnen.
3. Empfohlen - Löschen Sie die Autorisierung für die Verknüpfung der VPC mit der gehosteten Zone. Das Löschen der Autorisierung wirkt sich nicht auf die Verknüpfung aus, sondern verhindert nur, dass Sie die VPC künftig erneut mit der gehosteten Zone verknüpfen. Wenn Sie die gehostete Zone erneut mit der VPC verknüpfen möchten, müssen Sie die Schritte 1 und 2 dieses Verfahrens wiederholen.

   > **Important**
   >
   > Die `ListHostedZonesByVPC` gibt die gehosteten Zonen zurück, wenn eine VPC vorhanden ist, und die `GetHostedZone` API gibt die der Hosting-Zone VPCs zugeordnete Zone zurück. Diese berücksichtigen APIs nur die Zuordnung zwischen

gehosteter Zone und VPC, die über die `AssociateVPCWithHostedZone` API oder bei der Erstellung der privaten gehosteten Zone erstellt wurde. Wenn Sie eine vollständige Liste der Hosting-Zonenzuordnungen zu einer VPC wünschen, rufen Sie auch an ListProfileResourceAssociations.

> **Note**
>
> Informationen zur maximalen Anzahl der Autorisierungen, die Sie erstellen können, finden Sie unter Kontingente für Entitäten.

Trennung von einer privaten VPCs gehosteten Zone

Sie können die Amazon Route 53-Konsole verwenden, um die Verbindung zu einer privaten gehosteten Zone zu trennen VPCs . Dies veranlasst Route 53, die Weiterleitung von Datenverkehr unter Verwendung von Datensätzen in der gehosteten Zone für DNS-Abfragen, die aus der VPC stammen, zu beenden. Wenn beispielsweise die gehostete Zone example.com mit einer VPC verknüpft ist und Sie die Verknüpfung der gehosteten Zone von dieser VPC aufheben, stellt Route 53 die Auflösung von DNS-Abfragen für example.com oder einen der anderen Datensätze in der gehosteten Zone example.com ein.

> **Note**
>
> Sie können die Zuordnung der letzten VPC zu einer privaten gehosteten Zone nicht aufheben. Wenn Sie die Verknüpfung von dieser VPC aufheben möchten, müssen Sie der gehosteten Zone zunächst eine andere VPC zuordnen.

Um die Verbindung zu einer privaten VPCs Hosting-Zone zu trennen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie das Optionsfeld für die private gehostete Zone VPCs aus, zu der Sie die Verbindung zu einer oder mehreren Zonen trennen möchten.
4. Wählen Sie Bearbeiten aus.

5. Klicken Sie aufRemove VPC (VPC entfernen)Klicken Sie auf die VPC, die Sie von dieser gehosteten Zone trennen möchten.
6. Wählen Sie Save Changes (Änderungen speichern).

Löschen einer privaten gehosteten Zone

In diesem Abschnitt wird erläutert, wie Sie eine privat gehostete Zone mithilfe der Amazon-Route-53-Konsole löschen können.

Sie können eine privat gehostete Zone nur dann löschen, wenn keine Datensätze (abgesehen von den Standard-SOA- und NS-Datensätzen) vorhanden sind. Wenn Ihre gehostet Zone andere Datensätze enthält, müssen Sie diese löschen, bevor Sie Ihre gehostete Zone löschen können. Dadurch wird verhindert, dass Sie versehentlich eine gehostete Zone löschen, die noch Datensätze enthält.

Themen

Löschen von privaten gehosteten Zonen, die von einem anderen Dienst erstellt wurden

Wenn eine privat gehostete Zone von einem anderen Dienst erstellt wurde, können Sie diese nicht mit der Route 53-Konsole löschen. Stattdessen müssen Sie den entsprechenden Vorgang für den anderen Dienst verwenden:

- AWS Cloud Map— Um eine gehostete Zone zu löschen, die bei der AWS Cloud Map Erstellung eines privaten DNS-Namespace erstellt wurde, löschen Sie den Namespace. AWS Cloud Map löscht die gehostete Zone automatisch. Weitere Informationen finden Sie unter Löschen von Namespaces im AWS Cloud Map Entwicklerleitfaden.
- Amazon Elastic Container Service (Amazon ECS) Service Discovery - So löschen Sie eine privat gehostete Zone, die Amazon ECS erstellt hat, als Sie einen Dienst mithilfe der Dienst-Erkennung erstellt haben, löschen Sie die Amazon-ECS-Services, die den Namespace verwenden und löschen Sie den Namespace. Weitere Informationen finden Sie unter Angeben vertraulicher Daten im Amazon Elastic Container Service-Entwicklerhandbuch.

Löschen einer privat gehosteten Zone mit der Route 53-Konsole.

Um die Route 53-Konsole zu verwenden, löschen Sie eine privat gehostete Zone, und führen Sie folgende Schritte aus.

Löschen einer privat gehosteten Zone mit der Route 53-Konsole.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Vergewissern Sie sich, dass die gehostete Zone, die Sie löschen möchten, nur einen NS- und einen SOA-Datensatz enthält. Enthält sie zusätzliche Datensätze, löschen Sie diese:

   a. Klicken Sie auf den Namen der gehosteten Zone, die Sie löschen möchten.

   b. Klicken Sie auf der Seite Record, wenn die Liste der Datensätze irgendwelche Datensätze enthält, für die der Wert der Spalte Type ein anderer ist als NS oder SOA, auf die entsprechende Zeile, und wählen Sie Delete.

      Um mehrere aufeinander folgende Datensätze auszuwählen, wählen Sie die erste Zeile aus, halten Sie die Umschalttaste gedrückt, und klicken Sie dann auf die letzte Zeile. Um mehrere nicht aufeinander folgende Datensätze auszuwählen, wählen Sie die erste Zeile aus, halten Sie die Strg-Taste gedrückt, und klicken Sie dann auf die gewünschten Zeilen.
3. Wählen Sie auf der Seite Hosted Zones die Zeile für die gehostete Zone aus, die Sie löschen möchten.
4. Wählen Sie Löschen aus.
5. Geben Sie den Bestätigungsschlüssel ein und wählen Sie Delete (Löschen) aus.

VPC-Berechtigungen

VPC-Berechtigungen verwenden die Richtlinienbedingung Identity and Access Management (IAM), damit Sie detaillierte Berechtigungen für die VPCs Verwendung von Associate VPCWith HostedZone, Disassociate VPCFrom HostedZone, Create VPCAssociation Authorization, Delete VPCAssociation Authorization und VPC festlegen können. CreateHostedZoneListHostedZonesBy APIs

Mit der IAM-Richtlinienbedingung können Sie anderen `route53:VPCs` Benutzern detaillierte Administratorrechte gewähren. AWS Auf diese Weise können Sie jemandem die Berechtigung erteilen, eine gehostete Zone zuzuordnen, die Hosting-Zone von ihr zu trennen, eine VPC-Zuordnungsautorisierung zu erstellen, die VPC-Zuordnungsautorisierung für zu löschen, eine gehostete Zone zu erstellen oder gehostete Zonen aufzulisten für:

- Eine einzelne VPC.
- Alle VPCs innerhalb derselben Region.
- Mehrfach VPCs.

Weitere Informationen zu VPC-Berechtigungen finden Sie unterVerwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

Informationen zur Authentifizierung von AWS Benutzern finden Sie unterAuthentifizierung mit Identitäten. Informationen zur Steuerung des Zugriffs auf Route 53-Ressourcen finden Sie unter. Zugriffskontrolle

Migrieren einer Hosting-Zone auf ein anderes Konto AWS

Folgen Sie diesen empfohlenen Schritten AWS-Konto, wenn Sie eine Hosting-Zone in eine andere migrieren.

Diese Schritte eignen sich am besten für Hosting-Zonen mit seltenen Datensatzänderungen. Beachten Sie bei Hosting-Zonen mit häufigen Datensatzaktualisierungen Folgendes:

- Aktualisieren Sie während der Migration keine Ressourceneinträge.
- Veröffentlichen Sie Änderungen an den Ressourceneinträgen sowohl in alten als auch in neuen Hosting-Zonen, nachdem die Delegierung übertragen wurde.

Voraussetzungen

Installieren oder aktualisieren Sie AWS CLI:

Informationen zum Herunterladen, Installieren und Konfigurieren von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI

> **Note**
>
> Konfigurieren Sie die CLI so, dass Sie einsatzbereit ist, wenn Sie sowohl das Konto, über das die gehostete Zone erstellt wurde, als auch das Konto verwenden, zu dem die gehostete Zone migriert wird. Weitere Informationen finden Sie unter Konfigurieren der im AWS Command Line Interface -Benutzerhandbuch.

Wenn Sie die bereits verwenden AWS CLI, empfehlen wir Ihnen, auf die neueste Version der CLI zu aktualisieren, damit die CLI-Befehle die neuesten Route 53-Funktionen unterstützen.

Themen

Schritt 1: Bereiten Sie sich auf die Migration vor

Die Vorbereitungsschritte helfen Ihnen dabei, die mit der Migration einer gehosteten Zone verbundenen Risiken zu minimieren.

1. Überwachen Sie die Verfügbarkeit der Zone

Sie können die Zone auf die Verfügbarkeit Ihrer Domänennamen überwachen. Auf diese Weise können Sie alle Probleme beheben, die zu einem Rollback der Migration führen könnten. Mithilfe der Protokollierung CloudWatch oder Abfrage können Sie überwachen, ob Ihre Domainnamen mit dem meisten Traffic betroffen sind. Für weitere Informationen zum Einrichten einer Abfrage-Protokollierung siehe Amazon Route 53 überwachen.

Die Überwachung kann über ein Shell-Skript oder über einen Drittanbieterdienst erfolgen. Dies sollte jedoch nicht das einzige Signal sein, anhand dessen festgestellt werden kann, ob ein Rollback erforderlich ist, da Sie möglicherweise auch Feedback von Ihren Kunden erhalten, wenn eine Domain nicht verfügbar ist.

2. Senken Sie die TTL-Einstellung

Die TTL-Einstellung (Time-to-live, Gültigkeitsdauer) für einen Datensatz gibt an, wie lange DNS-Resolver den Datensatz zwischenspeichern und die zwischengespeicherten Informationen verwenden sollen. Wenn die TTL abgelaufen ist, sendet ein Resolver eine weitere Abfrage an den DNS-Dienstanbieter für eine Domäne, um die neuesten Informationen zu erhalten.

Die typische TTL-Einstellung für den NS Datensatz ist 172 800 Sekunden oder 2 Tage. Der NS-Datensatz listet die Namenserver auf, die das Domain Name System (DNS) verwenden kann, um Informationen zum Weiterleiten des Datenverkehrs für Ihre Domäne abzurufen. Wenn Sie die TTL für den NS-Eintrag sowohl bei Ihrem aktuellen DNS-Dienstanbieter als auch bei Route 53 senken, werden die Ausfallzeiten für Ihre Domain reduziert, falls Sie bei der Migration von DNS zu Route 53 ein Problem feststellen. Wenn Sie die TTL nicht senken, ist Ihre Domäne bis zu zwei Tage im Internet nicht verfügbar, wenn ein Fehler auftritt.

Um die TTL zu senken

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich die Option Gehostete Zonen aus.
3. Wählen Sie den Namen der gehosteten Zone aus.
4. Wählen Sie den NS-Eintrag und dann im Bereich Datensatzdetails die Option Datensatz bearbeiten aus.
5. Ändern Sie den Wert TTL (Seconds). Wir empfehlen, einen Wert zwischen 60 Sekunden und 900 Sekunden (15 Minuten) anzugeben.
6. Wählen Sie Speichern.

3. Entfernen Sie den DS-Eintrag aus der übergeordneten Zone (wenn Sie DNSSEC konfiguriert haben)

Wenn Sie DNSSEC für Ihre Domäne konfiguriert haben, entfernen Sie den Eintrag Delegation Signer (DS) aus der übergeordneten Zone, bevor Sie Ihre Domäne zu Route 53 migrieren.

Wenn die übergeordnete Zone über Route 53 gehostet wird, finden Sie Löschen von öffentlichen Schlüsseln für eine Domäne weitere Informationen unter. Wenn die übergeordnete Zone bei einem anderen Registrar gehostet wird, wenden Sie sich an diesen, um den DS-Eintrag zu entfernen.

Route 53 unterstützt derzeit nicht die Migration der DNSSEC-Einstellung. Daher müssen Sie die DNSSEC-Validierung, die vor der Migration für Ihre Domain durchgeführt wurde, deaktivieren, indem Sie den DS-Eintrag aus der übergeordneten Zone entfernen. Nach der Migration können Sie die

DNSSEC-Validierung wieder aktivieren, indem Sie DNSSEC in der neuen Hosting-Zone konfigurieren und den entsprechenden DS-Eintrag zur übergeordneten Zone hinzufügen.

4. Stellen Sie sicher, dass keine anderen laufenden Operationen von der migrierenden Hosting-Zone abhängen

Einige Vorgänge hängen von der DNS-Auflösung in der migrierenden Hostzone ab. Beispielsweise müssen bei der TLS/SSL Zertifikatserneuerung möglicherweise Änderungen am DNS-Eintrag vorgenommen werden, und der Anbieter versucht, den DNS-Eintrag als Validierungsmethode aufzulösen. Vor der Migration sollten Sie sicherstellen, dass kein anderer Vorgang ausgeführt wird, um unerwartete Auswirkungen der Migration der Hosting-Zone zu vermeiden.

Schritt 2: Erstellen der neuen gehosteten Zone

Erstellen Sie die neue Hosting-Zone in dem Konto, zu dem Sie die Hostzone migrieren möchten.

Wählen Sie die Registerkarte mit den Anweisungen für die Konsole AWS CLI oder.

- CLI
- Konsole

CLI

Geben Sie den folgenden Befehl ein:

```
aws route53 create-hosted-zone \
            --name $hosted_zone_name \
            --caller-reference $unique_string
```

Weitere Informationen finden Sie unter create-hosted-zone.

Console

So erstellen Sie die neue gehostete Zone mit einem anderen Konto

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   Melden Sie sich mit den Anmeldeinformationen für das Konto an, zu dem Sie die gehostete Zone migrieren möchten.

2. Erstellen Sie eine gehostete Zone. Weitere Informationen finden Sie unter Erstellen einer öffentlichen gehosteten Zone.
3. Notieren Sie sich die ID der gehosteten Zone. In einigen Fällen benötigen Sie diese Informationen zu einem späteren Zeitpunkt.
4. Melden Sie sich bei der Route 53-Konsole ab.

Senken Sie die NS-TTL auch in der neuen Zone, ähnlich der Einstellung „Niedrigere TTL“ in Vorbereitung. Schritt 1, Senken Sie die TTL-Einstellung.

Schritt 3: (Optional) Migrieren Sie die Zustandsprüfungen

Sie können DNS-Einträge im neuen Konto den Route 53-Zustandsprüfungen des Kontos zuordnen, von dem Sie migrieren. Um eine Route 53-Zustandsprüfung zu migrieren, müssen Sie in Ihrem neuen Konto neue Zustandsprüfungen mit derselben Konfiguration wie Ihre vorhandenen erstellen. Weitere Informationen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

Schritt 4: Migrieren Sie Datensätze von der alten Hosting-Zone zur neuen Hosting-Zone

Sie können Datensätze von einem AWS-Konto zu einem anderen migrieren, indem Sie die Konsole oder die verwenden AWS CLI.

Console

Wenn Ihre Zone nur wenige Datensätze enthält, können Sie erwägen, die Route 53-Konsole zu verwenden, um die Datensätze in Ihrer alten Zone aufzulisten, sie zu notieren und sie in der neuen Zone zu erstellen. Wenn Sie den Integritätscheck migriert habenSchritt 3: (Optional) Migrieren Sie die Zustandsprüfungen, sollten Sie beim Erstellen der Datensätze in der neuen Hosting-Zone die neue Integritätsprüfungs-ID angeben. Weitere Informationen finden Sie unter den folgenden Themen:

- Auflisten von Datensätzen
- Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole
- Konfigurieren von DNS Failover

Sie sollten die NS-TTL auch in der neuen Zone senken, ähnlich der Einstellung „Niedrigere TTL“ in Schritt 1.

CLI

Wenn Ihre Zone eine große Anzahl von Datensätzen enthält, können Sie die Datensätze, die Sie migrieren möchten, in eine Datei exportieren, die Datei bearbeiten und dann die bearbeitete Datei verwenden, um Datensätze in der neuen Hosting-Zone zu erstellen. Das folgende Verfahren verwendet AWS CLI-Befehle, obwohl zu diesem Zweck auch Tools von Drittanbietern verfügbar sind.

1. Führen Sie den folgenden Befehl aus:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
   ```

   Beachten Sie Folgendes:

   - Geben Sie für *hosted-zone-id* die ID der alten Hosting-Zone an, die die Datensätze enthält, die Sie migrieren möchten.
   - Geben Sie für *path-to-output-file* den Verzeichnispfad und den Dateinamen an, in dem Sie die Ausgabe speichern möchten.
   - Das >-Zeichen sendet die Ausgabe an die angegebene Datei.
   - Die verarbeitet AWS CLI automatisch die Paginierung für Hosting-Zonen, die mehr als 100 Datensätze enthalten. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter Verwenden der Paginierungsoptionen der AWS Befehlszeilenschnittstelle.

     Wenn Sie eine andere programmatische Methode zum Auflisten von Datensätzen verwenden, z. B. einen der AWS SDKs, können Sie maximal 100 Datensätze pro Ergebnisseite abrufen. Wenn die gehostete Zone mehr als 100 Datensätze enthält, müssen Sie mehrere Anforderungen zur Auflistung aller Datensätze übermitteln.

   Erstellen Sie eine Kopie dieser Ausgabe. Nachdem Sie Datensätze in der neuen Hosting-Zone erstellt haben, empfehlen wir, den AWS CLI `list-resource-record-sets` Befehl für die neue Hosting-Zone auszuführen und die beiden Ausgaben zu vergleichen, um sicherzustellen, dass alle Datensätze erstellt wurden.
2. Bearbeiten Sie die Datensätze, die Sie migrieren möchten.

Bearbeiten Sie die exportierte Datei, bevor Sie sie mit dem `change-resource-record-sets` Befehl verwenden können. Sie können diese Änderungen mithilfe der Such- und Ersetzungsfunktion in einem Texteditor vornehmen.

> **Note**
>
> Die folgenden Schritte beschreiben die manuelle Bearbeitung mit einem Texteditor. Fortgeschrittene Benutzer können diese Transformationen mithilfe von programmatischen Tools wie jq, Python oder anderen Skriptsprachen automatisieren.

Öffnen Sie eine Kopie der Datei, die Sie in Schritt 1 dieses Verfahrens erstellt haben und die die Datensätze enthält, die Sie migrieren möchten, und nehmen Sie die folgenden Änderungen vor:

- Ersetzen Sie das ResourceRecordSets Element oben in der Datei durch `Changes` Element.
- Optional — füge ein `Comment` Element hinzu.
- Löschen Sie die Zeilen, die sich auf die NS- und SOA-Einträge des Namens der gehosteten Zone beziehen. Die neue gehostete Zone verfügt bereits über diese Datensätze.
- Fügen Sie für jeden Datensatz ein Element `Action` und ein `ResourceRecordSets` Element hinzu und fügen Sie nach Bedarf öffnende und schließende Klammern (`{ }`) hinzu, damit der JSON-Code gültig ist.

  > **Note**
  >
  > Sie können einen JSON-Validator einsetzen, um sicherzustellen, dass alle Klammern an den erforderlichen Stellen vorhanden sind. Um einen Online-JSON-Validator zu finden, suchen Sie in Ihrem Browser nach „JSON-Validator“.

- Wenn die gehostete Zone Aliasse enthält, die sich auf andere Datensätze in derselben gehosteten Zone beziehen, nehmen Sie die folgenden Änderungen vor:
  - Ändern Sie die ID der gehosteten Zone in die ID der neuen gehosteten Zone.

> **Important**
>
> Wenn der Aliaseintrag auf eine andere Ressource verweist, z. B. auf einen Load Balancer, ändern Sie die Hosting-Zonen-ID nicht in die Hosting-Zonen-ID der Domain. Wenn Sie die Hosting-Zonen-ID versehentlich ändern, setzen Sie die Hosting-Zonen-ID auf die Hosting-Zonen-ID der Ressource selbst zurück, nicht auf die Hosting-Zonen-ID der Domain. Die ID der gehosteten Zone der Ressource befindet sich in der AWS Konsole, in der die Ressource erstellt wurde.

- Verschieben Sie die Alias-Datensätze an das Ende der Datei. Route 53 muss den Datensatz erstellen, auf den sich ein Alias-Datensatz bezieht, ehe es den Alias-Datensatz erstellen kann.

  > **Important**
  >
  > Wenn ein oder mehrere Alias-Datensätze auf andere Alias-Datensätze verweisen, müssen die Datensätze, die das Alias-Ziel darstellen, vor den referenzierenden Datensätzen aufgeführt werden. Beispiel: Wenn das Alias-Ziel für `alias.alias.example.com` `alias.example.com` ist, muss `alias.example.com` zuerst in der Datei aufgeführt werden.

  - Löschen Sie alle Alias-Datensätze, die Datenverkehr zu einer Datenverkehrsrichtlinien-Instance umleiten. Notieren Sie sich die Datensätze, sodass Sie sie zu einem späteren Zeitpunkt erneut erstellen können.
- Wenn Sie Integritätsprüfungen migriert habenSchritt 3: (Optional) Migrieren Sie die Zustandsprüfungen, ändern Sie die Datensätze, um sie der neu erstellten Zustandsprüfung IDs zuzuordnen.

Das folgende Beispiel zeigt die bearbeitete Version von Datensätzen für eine gehostete Zone für example.com. Der rote, kursive Text ist neu:

```
{
    "Comment": "string",
    "Changes": [
        {
            "Action": "CREATE",
```

```
            "ResourceRecordSet":{
                "ResourceRecords": [
                    {
                        "Value": "192.0.2.4"
                    },
                    {
                        "Value": "192.0.2.5"
                    },
                    {
                        "Value": "192.0.2.6"
                    }
                ],
                "Type": "A",
                "Name": "route53documentation.com.",
                "TTL": 300
            }
        },
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "AliasTarget": {
                    "HostedZoneId": "Z3BJ6K6RIION7M",
                    "EvaluateTargetHealth": false,
                    "DNSName": "s3-website-us-west-2.amazonaws.com."
                },
                "Type": "A",
                "Name": "www.route53documentation.com."
            }
        }
    ]
}
```

3. Teilen Sie große Dateien in kleinere Dateien auf

   Wenn Sie viele Datensätze haben oder Datensätze, die viele Werte enthalten (z. B. zahlreiche IP-Adressen), müssen Sie die Datei möglicherweise in mehrere kleinere Dateien aufteilen. Die Maximalwerte sind:

   - Eine Datei darf maximal 1 000 Datensätze enthalten.
   - Die maximale Gesamtlänge der Werte in allen `Value`-Elementen ist auf 32 000 Byte begrenzt.

4. Erstellen Sie Datensätze in der neuen Hosting-Zone

Geben Sie die folgende CLI ein:

```
aws route53 change-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
            --change-batch file://path-to-file-that-contains-records
```

Geben Sie die folgenden Werte an:

- Geben Sie für *new-hosted-zone-id* die ID der neuen gehosteten Zone an.
- Geben Sie für *path-to-file-that-contains-records* den Verzeichnispfad und den Dateinamen an, die Sie in den vorherigen Schritten bearbeitet haben.

Wenn Sie Alias-Datensätze gelöscht haben, mithilfe derer der Datenverkehr zu einer Datenverkehrsrichtlinien-Instance umgeleitet wird, erstellen Sie diese mit der Route 53-Konsole neu. Weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

Schritt 5: Vergleichen Sie Datensätze in den alten und neuen Hosting-Zonen

Um zu bestätigen, dass Sie alle Ihre Datensätze in der neuen Hosting-Zone erfolgreich erstellt haben, geben Sie den folgenden CLI-Befehl ein, um die Datensätze in der neuen Hosting-Zone aufzulisten und die Ausgabe mit der Liste der Datensätze aus der alten Hosting-Zone zu vergleichen.

```
aws route53 list-resource-record-sets \
            --hosted-zone-id new-hosted-zone-id \
            --output json > path-to-output-file
```

Geben Sie die folgenden Werte an:

- Geben Sie für *new-hosted-zone-id* die ID der neuen Hosting-Zone an.
- Geben Sie für *path-to-output-file* den Verzeichnispfad und den Dateinamen an, in dem Sie die Ausgabe speichern möchten. Verwenden Sie einen Dateinamen, der sich von dem Dateinamen unterscheidet, den Sie in Schritt 4 verwendet haben.

  Das >-Zeichen sendet die Ausgabe an die angegebene Datei.

Vergleichen Sie die Ausgabe mit der Ausgabe aus Schritt 4. Abgesehen von den Werten der NS- und SOA-Einträge und allen Änderungen, die Sie in Schritt 4 vorgenommen haben (z. B. unterschiedliche Hostingzonen IDs - oder Domainnamen), sollten die beiden Ausgaben identisch sein.

Wenn die Datensätze in der neuen Hosting-Zone nicht mit den Datensätzen in der alten Hosting-Zone übereinstimmen, gehen Sie wie folgt vor:

- Nehmen Sie kleinere Korrekturen über die Route 53-Konsole vor. Weitere Informationen finden Sie unter Bearbeiten von Datensätzen.
- Löschen Sie alle Datensätze außer den NS- und SOA-Datensätzen in der neuen Hosting-Zone, und wiederholen Sie den Vorgang in Schritt 4.

Schritt 6: Aktualisieren Sie die Domainregistrierung, um Nameserver für die neue Hosting-Zone zu verwenden

Wenn Sie mit der Migration der Datensätze in die neue Hosting-Zone fertig sind, ändern Sie die Nameserver für die Domainregistrierung so, dass sie die Nameserver für die neue Hosting-Zone verwenden. Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Service für eine bestehende Domain machen.

Wenn Ihre gehostete Zone verwendet wird — wenn Ihre Benutzer beispielsweise den Domainnamen verwenden, um eine Website aufzurufen oder auf eine Webanwendung zuzugreifen — sollten Sie weiterhin den Verkehr und die Verfügbarkeit der gehosteten Zone überwachen, einschließlich Website- oder Anwendungsverkehr, E-Mail usw.

- Wenn sich der Verkehr verlangsamt oder stoppt — Stellen Sie den Name-Service für die Domainregistrierung wieder auf die vorherigen Nameserver der alten Hosting-Zone um. Ergründen Sie anschließend, was schiefgelaufen ist.
- Wenn der Verkehr nicht beeinträchtigt wird — Fahren Sie mit dem nächsten Schritt fort.

Schritt 7: Ändern Sie die TTL für den NS-Eintrag wieder auf einen höheren Wert

Ändern Sie in der neuen Hosting-Zone die TTL für den NS-Eintrag auf einen typischeren Wert, z. B. 172800 Sekunden (zwei Tage). Dadurch wird die Latenz für Ihre Benutzer verbessert, da sie nicht so oft darauf warten müssen, dass DNS-Resolver eine Abfrage für die Namenserver Ihrer Domäne senden.

Um die TTL zu ändern

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich die Option Gehostete Zonen aus.
3. Wählen Sie den Namen der gehosteten Zone aus.
4. Wählen Sie den NS-Eintrag und dann im Bereich Datensatzdetails die Option Datensatz bearbeiten aus.
5. Ändern Sie den Wert von TTL (Sekunden) auf die Anzahl der Sekunden, für die DNS-Resolver die Namen der Nameserver für Ihre Domain zwischenspeichern sollen. Wir empfehlen einen Wert von 172 800 Sekunden.
6. Wählen Sie Speichern.

Schritt 8: Aktivieren Sie die DNSSEC-Signatur erneut und richten Sie die Vertrauenskette ein (falls erforderlich)

Sie können die DNSSEC-Signatur in zwei Schritten wieder aktivieren:

1. Aktivieren Sie die DNSSEC-Signatur für Route 53 und fordern Sie Route 53 auf, einen Key Signing Key (KSK) auf der Grundlage einer vom Kunden verwalteten Schlüsseleingabe zu erstellen. AWS Key Management Service
2. Erstellen Sie eine Vertrauenskette für die gehostete Zone, indem Sie der übergeordneten Zone einen DS-Eintrag (Delegation Signer) hinzufügen, sodass DNS-Antworten mit vertrauenswürdigen kryptografischen Signaturen authentifiziert werden können.

Detaillierte Anweisungen finden Sie unter Aktivieren der DNSSEC-Signierung und Aufbau einer Vertrauenskette.

Schritt 9: (Optional) Löschen Sie die alte Hosting-Zone

Wenn Sie sicher sind, die alte gehostete Zone nicht mehr zu benötigen, können Sie diese löschen. Detaillierte Anweisungen finden Sie unter Löschen einer öffentlichen gehosteten Zone.

> **Important**
>
> Löschen Sie die alte gehostete Zone bzw. Datensätze in dieser gehosteten Zone nicht während mindestens 48 Stunden, nachdem Sie die Domänenregistrierung aktualisiert

haben, damit für die neue gehostete Zone Nameserver verwendet werden. Wenn Sie die alte gehostete Zone löschen, bevor die DNS-Resolver die Verwendung der Datensätze in dieser gehosteten Zone einstellen, könnte Ihre Domäne im Internet nicht verfügbar sein, bis Resolver die neue gehostete Zone verwenden.

Arbeiten mit Datensätzen

Nach der Erstellung einer gehosteten Zone für Ihre Domain (z. B. example.com) erstellen Sie Datensätze, um dem Domain Name System (DNS) mitzuteilen, wie der Datenverkehr für diese Domain weitergeleitet werden soll.

Sie können beispielsweise Datensätze erstellen, aufgrund derer DNS Folgendes tut:

- Internetdatenverkehr für example.com wird zur IP-Adresse eines Hosts in Ihrem Rechenzentrum weitergeleitet.
- E-Mails für diese Domain (ichiro@example.com) werden zu einem Mail-Server (mail.example.com) weitergeleitet.
- Der Datenverkehr für eine Subdomain mit dem Namen operations.tokyo.example.com wird zur IP-Adresse eines anderen Hosts weitergeleitet.

Jeder Datensatz enthält den Namen einer Domain oder einer Subdomain, einen Datensatztyp (ein Datensatz mit dem Typ MX leitet beispielsweise E-Mail-Nachrichten weiter) und andere Informationen bezüglich des Datensatztyps (den Hostnamen von einem oder mehreren Mail-Servern und eine Priorität für jeden Server für MX-Datensätze). Weitere Informationen zu den verschiedenen Arten von Datensätzen finden Sie unter Unterstützte DNS-Datensatztypen.

Der Name jedes Datensatzes in einer gehosteten Zone muss mit dem Namen der gehosteten Zone enden. Die gehostete Zone example.com kann beispielsweise Datensätze für die Subdomains www.example.com und accounting.tokyo.example.com enthalten, aber keine Datensätze für eine Subdomain wie www.example.ca.

> **Note**
>
> Um Datensätze für komplexe Routing-Konfigurationen zu erstellen, können Sie auch den Visual Editor Traffic Flow verwenden und die Konfiguration als Verkehrsrichtlinie speichern. Sie können dann die Datenverkehrsrichtlinie mit einem oder mehreren Domainnamen (z. B.

example.com) oder Subdomainnamen (z. B. www.example.com) in derselben gehosteten Zone oder in mehreren gehosteten Zonen verknüpfen. Außerdem können Sie ein Rollback der Aktualisierungen durchführen, wenn die neue Konfiguration sich nicht wie erwartet verhält. Weitere Informationen finden Sie unter Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr.

In Amazon Route 53 werden keine Gebühren für Datensätze berechnet, die Sie einer gehosteten Zone hinzufügen. Informationen zu Höchstwerten für die Anzahl der Datensätze, die Sie in einer gehosteten Zone erstellen können, finden Sie unter Kontingente.

Themen

Auswählen einer Routing-Richtlinie

Wenn Sie einen Datensatz erstellen, müssen Sie eine Routing-Richtlinie auswählen, die bestimmt, wie Amazon Route 53 auf Abfragen reagiert:

- Einfache Routing-Richtlinie – wird für eine einzelne Ressource verwendet, die eine bestimmte Funktion für Ihre Domain übernimmt, beispielsweise ein Webserver, der für die Inhalte für die Website example.com zuständig ist. Sie können einfaches Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.
- Failover-Routing-Richtlinie – wird verwendet, wenn Sie ein Aktiv-Passiv-Failover konfigurieren möchten. Sie können einfaches Failover-Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.

- Geolocation-Routing-Richtlinie – wird verwendet, wenn Sie den Datenverkehr auf Basis des Standorts Ihrer Benutzer weiterleiten möchten. Sie können einfaches Geolocation-Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.
- Routing-Richtlinie auf der Grundlage der geografischen Nähe: Wird verwendet, wenn Sie Datenverkehr auf Basis des Standorts Ihrer Ressourcen weiterleiten möchten und optional Datenverkehr von Ressourcen an einem Standort auf Ressourcen an einem anderen Standort verlagern möchten. Sie können Geoproximity-Routing verwenden, um Datensätze in einer privaten, gehosteten Zone zu erstellen.
- Latenz-Routing-Richtlinie — Verwenden Sie diese Richtlinie, wenn Sie über mehrere Ressourcen verfügen AWS-Regionen und den Datenverkehr in die Region weiterleiten möchten, die die beste Latenz bietet. Sie können Latenz-Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.
- IP-basierte Routing-Richtlinie: Wird verwendet, wenn Sie den Datenverkehr auf Basis des Standorts Ihrer Benutzer weiterleiten möchten und die IP-Adressen haben, von denen der Datenverkehr stammt.
- Mehrwertige Antwort-Routing-Richtlinie – wird verwendet, wenn Sie möchten, dass Route 53 mit bis zu acht zufällig ausgewählten und fehlerfreien Datensätzen auf DNS-Abfragen antwortet. Sie können mehrwertiges Antwort-Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.
- Gewichtete Routing-Richtlinie – wird verwendet, um Datenverkehr in festgelegten Proportionen zu mehreren Ressourcen weiterzuleiten. Sie können gewichtetes Routing verwenden, um Datensätze in einer privat gehosteten Zone zu erstellen.

Themen

Einfaches Routing

Einfaches Routing ermöglicht die Konfiguration von Standard-DNS-Datensätzen ohne spezielles Route-53-Routing, wie z. B. gewichtet oder Latenz. Bei einfachem Routing leiten Sie den Datenverkehr normalerweise an eine einzelne Ressource weiter, beispielsweise an einen Webserver für Ihre Website.

Sie können einfaches Routing für Datensätze in einer privat gehosteten Zone verwenden.

Wenn Sie die einfache Routing-Richtlinie in der und Route-53-Konsole auswählen, können Sie nicht mehrere Datensätze mit demselben Namen und desselben Typs erstellen. Sie können jedoch mehrere Werte im selben Datensatz angeben, z. B. mehrere IP-Adressen. (Wenn Sie die einfache Routing-Richtlinie für einen Aliaseintrag wählen, können Sie nur eine AWS Ressource oder einen Datensatz in der aktuellen Hosting-Zone angeben.) Wenn Sie mehrere Werte in einem Datensatz angeben, gibt Route 53 alle Werte in zufälliger Reihenfolge an den rekursiven Resolver zurück, und der Resolver gibt die Werte an den Client (z. B. einen Webbrowser) zurück, der die DNS-Abfrage gesendet hat. Der Client wählt dann einen Wert aus und sendet die Abfrage erneut. Mit einer einfachen Routing-Richtlinie können Sie zwar mehrere IP-Adressen angeben, diese IP-Adressen werden jedoch nicht auf den Zustand überprüft.

Informationen zu Werten, die Sie angeben, wenn Sie die einfache Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für einfache Datensätze
- Spezifische Werte für einfache Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Failover-Routing

Failover-Routing ermöglicht es Ihnen, Datenverkehr zu einer Ressource weiterzuleiten, wenn die Ressource fehlerfrei ist, oder zu einer anderen Ressource, wenn es bei der ersten Ressource ein Problem gibt. Die primären und sekundären Datensätze können Datenverkehr zu allem weiterleiten, von einem als Website konfigurierten Amazon-S3-Bucket bis hin zu einer komplexen Datensatzstruktur. Weitere Informationen finden Sie unter Aktiv/Passiv-Failover.

Sie können Failover-Routing für Datensätze in einer privat gehosteten Zone verwenden.

Informationen zu Werten, die Sie angeben, wenn Sie die einfache Failover-Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für Failover-Datensätze
- Spezifische Werte für Failover-Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Geolocation-Routing

Geolocation-Routing ermöglicht es Ihnen, die angesteuerten Ressourcen auf Basis des geographischen Standorts Ihrer Benutzer auszuwählen, also auf Basis des Standorts, von dem aus DNS-Abfragen gesendet werden. Sie können beispielsweise alle Abfragen aus Europa an einen Elastic Load Balancing Load Balancer in der Region Frankfurt weiterleiten.

Wenn Sie Geolocation-Routing verwenden, können Sie Ihre Inhalte lokalisieren und Ihre Website ganz oder teilweise in der Sprache Ihrer Benutzer präsentieren. Außerdem können Sie mit dem Geolocation-Routing die Verteilung von Inhalten auf Standorte beschränken, für die Sie Verteilungsrechte besitzen. Eine weitere mögliche Verwendung besteht darin, die Last auf vorhersehbare easy-to-manage Weise zwischen den Endpunkten auszugleichen, sodass jeder Benutzerstandort konsistent an denselben Endpunkt weitergeleitet wird.

Sie können geografische Standorte nach Kontinent, Land oder Staat in den Vereinigten Staaten angeben. Wenn Sie getrennte Datensätze für sich überschneidende geografische Regionen erstellen, z. B. einen Datensatz für Nordamerika und einen für Kanada, hat die kleinste geographische Region Priorität. Auf diese Weise können Sie einige Abfragen für einen Kontinent zu einer Ressource leiten und Abfragen für ausgewählte Länder auf diesem Kontinent zu einer anderen Ressource leiten. (Eine Liste der Länder auf jedem Kontinent finden Sie unter Ort.)

Geolocation funktioniert durch Mapping von IP-Adressen zu Standorten. Einige IP-Adressen werden jedoch nicht auf geografische Standorte abgebildet, sodass, selbst wenn Sie Datensätze für Geolokationen erstellen, die alle sieben Kontinente abdecken, Amazon Route 53 einige DNS-Abfragen von Standorten erhält, die es nicht identifizieren kann. Sie können ein Standarddatensatz erstellen, der für Abfragen von IP-Adressen angewendet wird, die keinem Standort zugeordnet sind, und für Abfragen von Standorten, für die Sie keine Geolocation-Datensätze erstellt haben. Wenn Sie keinen Standarddatensatz erstellen, gibt Route 53 „keine Antwort“ für Abfragen von diesen Standorten zurück.

Sie können einfaches Geolocation-Routing für Datensätze in öffentlich und privat gehosteten Zonen verwenden.

Weitere Informationen finden Sie unter Wie Amazon Route 53 EDNS0 zur Schätzung des Standorts eines Benutzers nutzt.

Informationen zu Werten, die Sie angeben, wenn Sie die einfache Geolocation-Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für Geolocation-Datensätze
- Spezifische Werte für Geolocation-Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Geolocation-Routing in privat gehosteten Zonen

Für privat gehostete Zonen antwortet Route 53 auf DNS-Abfragen, die auf AWS-Region der VPC basieren, von der die Anfrage stammt. Eine Liste von AWS-Regionen finden Sie unter Regionen und Zonen im EC2 Amazon-Benutzerhandbuch.

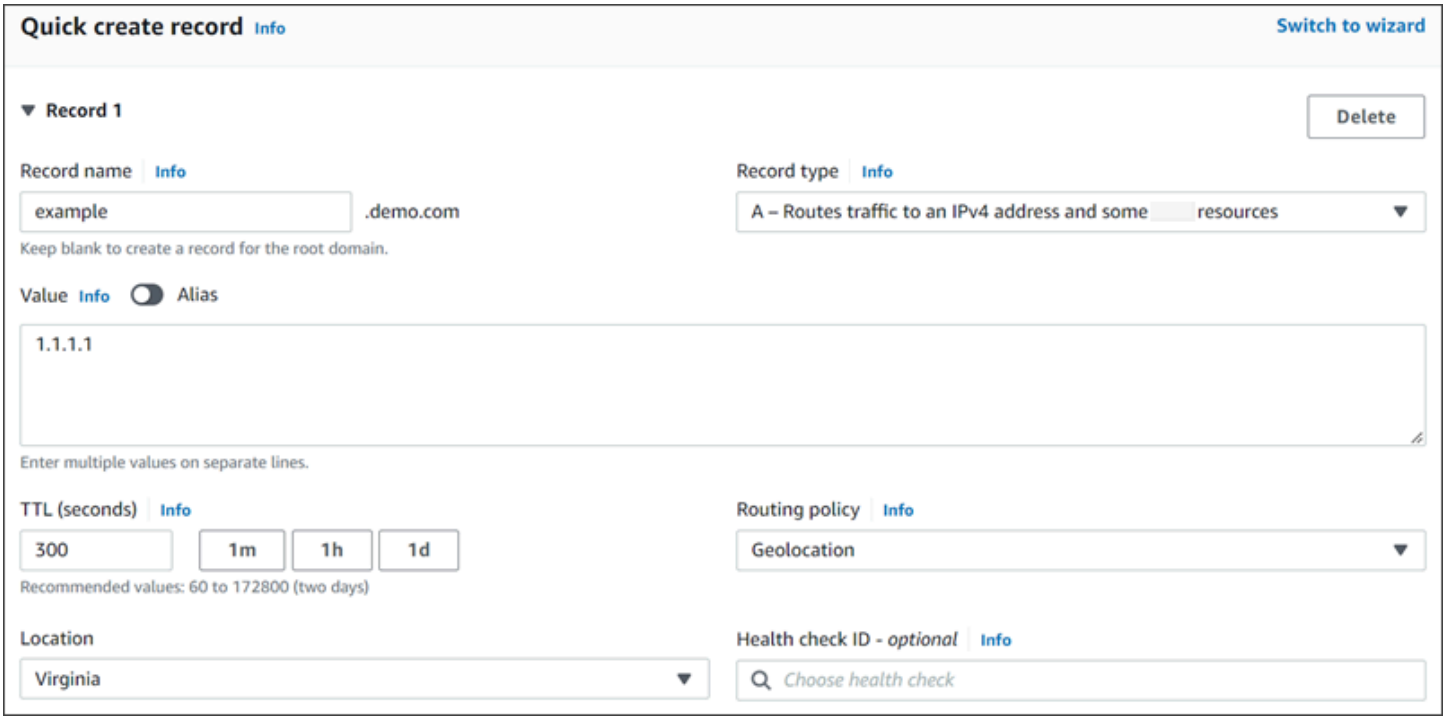
Wenn die DNS-Abfrage von einem On-Premises-Teil eines Hybridnetzwerks stammt, wird davon ausgegangen, dass sie aus der AWS-Region stammt, in der sich die VPC befindet.

Wenn Sie Integritätsprüfungen einbeziehen, können Sie Standarddatensätze erstellen für:

- IP-Adressen, die keinen geografischen Standorten zugeordnet sind.
- DNS-Abfragen, die von Standorten stammen, für die Sie keine Geolocation-Datensätze erstellt haben.

Wenn der Geolocation-Datensatz für die Region der DNS-Abfrage nicht ordnungsgemäß ist, wird der Standarddatensatz zurückgegeben (falls er fehlerfrei ist).

In der Beispielkonfiguration in der folgenden Abbildung werden DNS-Abfragen, die von einem us-east-1 AWS-Region (Virginia) kommen, an den 1.1.1.1-Endpunkt weitergeleitet.



Geoproximity-Routing

Mithilfe der Weiterleitung auf der Grundlage der geografischen Nähe kann Amazon Route 53 den Datenverkehr auf der Grundlage des geografischen Standorts Ihrer Benutzer und Ressourcen an Ihre Ressourcen weiterleiten. Es leitet den Verkehr an die nächstgelegene verfügbare Ressource weiter. Sie können optional auch mehr oder weniger Datenverkehr an eine bestimmte Ressource weiterleiten, indem Sie einen Wert angeben, der als Bias bezeichnet wird. Ein Bias-Wert vergrößert oder verkleinert die geografische Region, aus der Datenverkehr an eine Ressource weitergeleitet wird.

Sie erstellen Regeln für die geografische Nähe für Ihre Ressourcen und geben für jede Regel einen der folgenden Werte an:

- Wenn Sie AWS Ressourcen verwenden, geben Sie die AWS-Region oder die lokale Zonengruppe an, in der Sie die Ressource erstellt haben.
- Wenn Sie Ressourcen verwenden, die keine AWS Ressourcen sind, geben Sie den Breiten- und Längengrad der Ressource an.

Um AWS Local Zones verwenden zu können, müssen Sie sie zuerst aktivieren. Weitere Informationen finden Sie im Benutzerhandbuch zu AWS Local Zones unter Erste Schritte mit Local Zones.

Weitere Informationen zum Unterschied zwischen AWS-Regionen und Local Zones finden Sie unter Regionen und Zonen im EC2 Amazon-Benutzerhandbuch.

Um optional die Größe der geografischen Region zu ändern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie für den Bias-Wert den gültigen Wert an:

- Um die Größe der geografischen Region zu erweitern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie für den Bias-Wert eine positive Ganzzahl von 1 bis 99 an. Route 53 verkleinert die Größe der angrenzenden Regionen.
- Um die Größe der geografischen Region zu verkleinern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie einen negativen Bias-Wert zwischen -1 und -99 an. Route 53 erweitert die Größe der angrenzenden Regionen.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

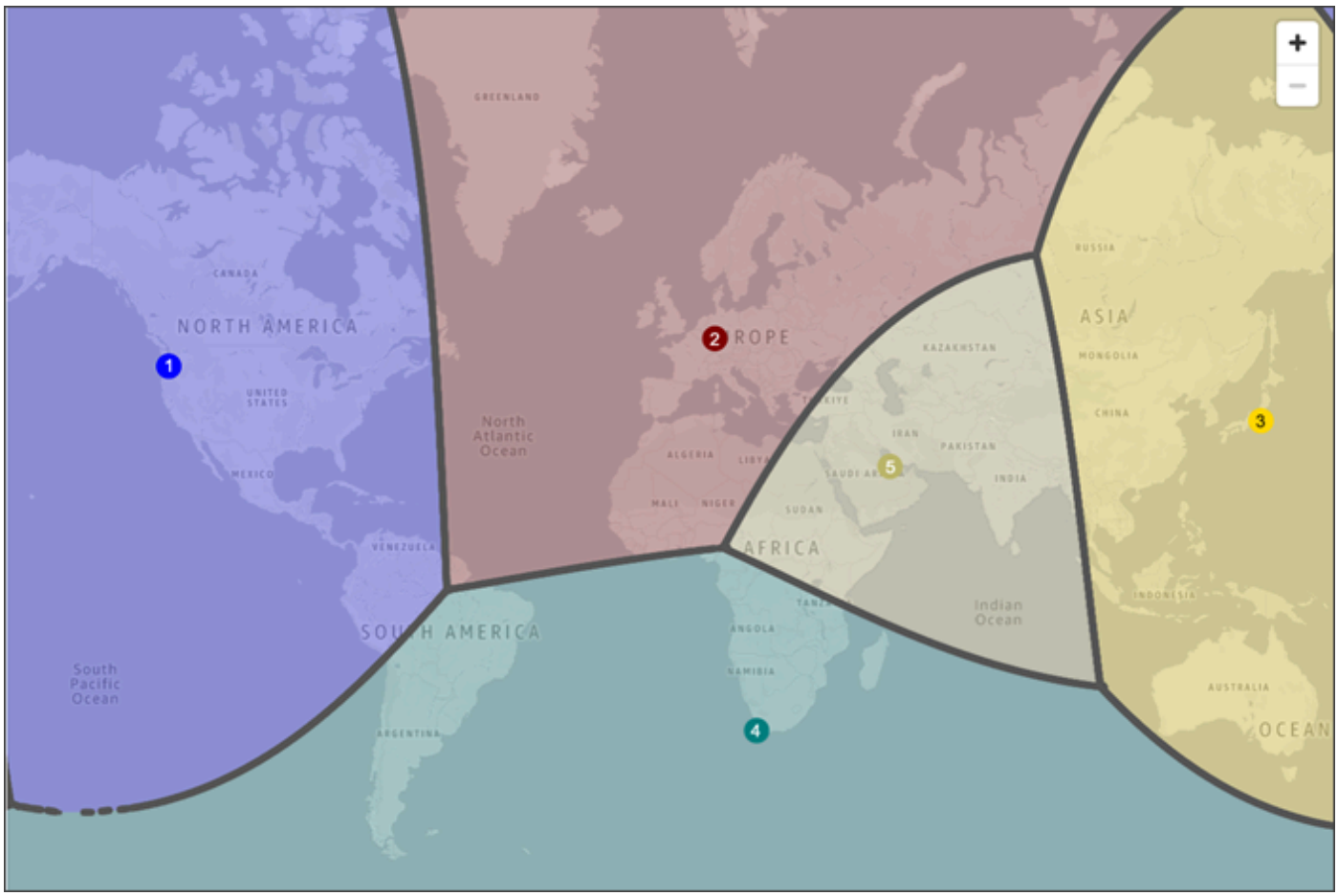
- New console
- Alte Konsole

New console

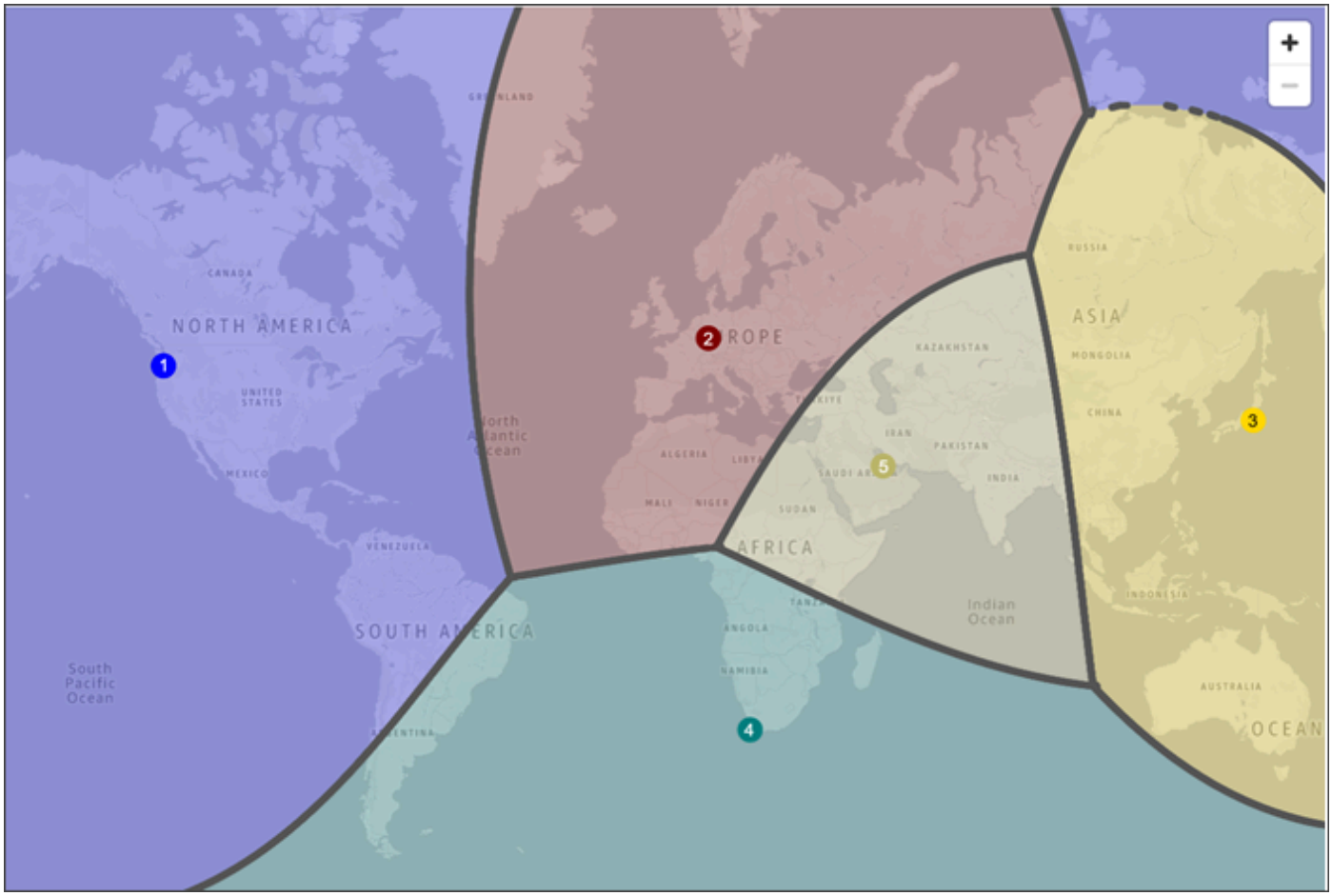
Die folgende Karte zeigt vier AWS-Regionen (nummeriert von 1 bis 5):

1. USA West (Oregon)
2. Europa (Frankfurt)
3. Asien-Pazifik (Tokio)
4. Afrika (Kapstadt)
5. Middle East (Bahrain)

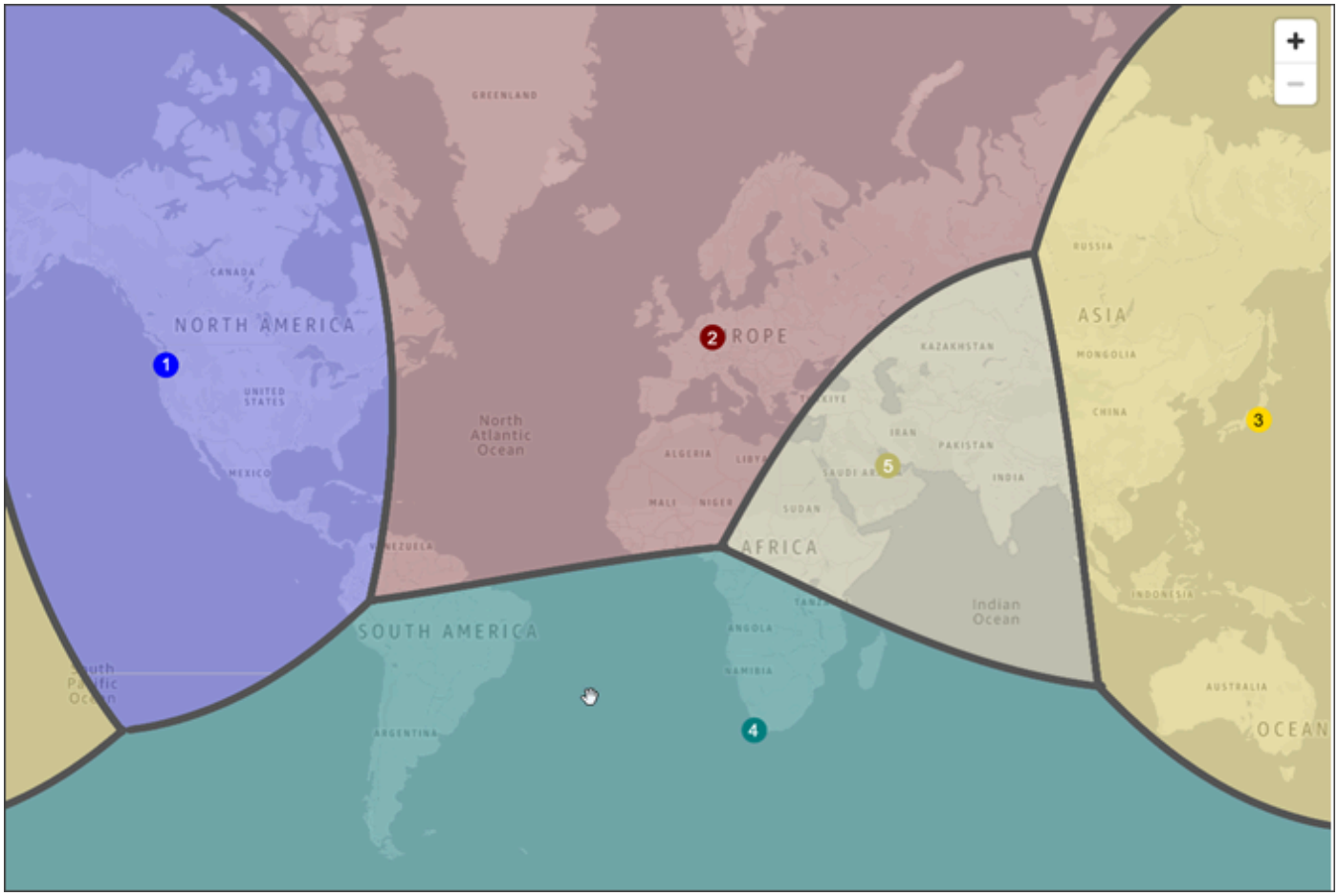
> **Note**
>
> Die Karten sind nur mit Traffic Flow verfügbar.



Die folgende Karte zeigt, was passiert, wenn Sie für die Region USA West (Oregon) (Nummer 1 auf der Karte) eine Abweichung von +25 hinzufügen. Der Verkehr wird aus einem größeren Teil Nordamerikas und aus ganz Südamerika als zuvor zu der Ressource in dieser Region geleitet.



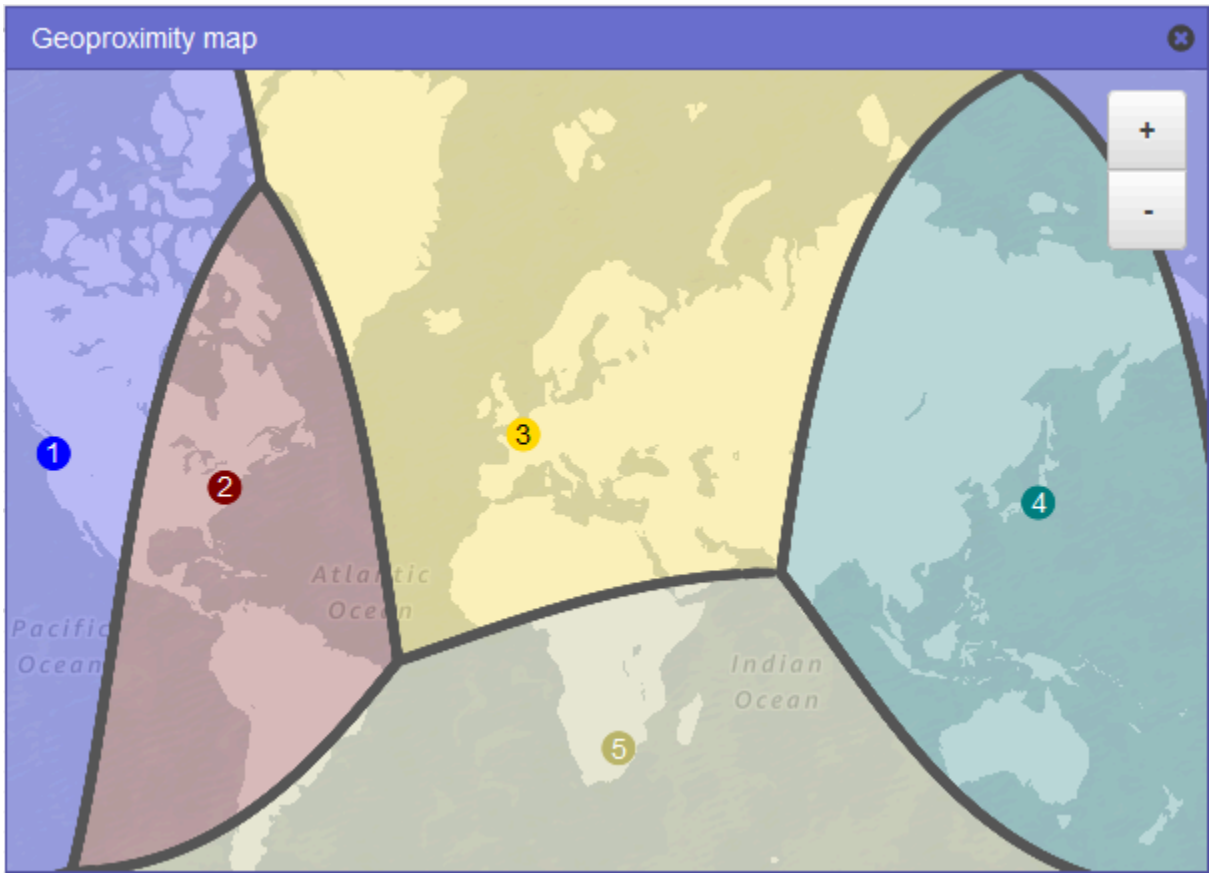
Die folgende Karte zeigt, was passiert, wenn Sie die Tendenz für die Region USA West (Oregon) auf -25 ändern. Der Verkehr wird aus kleineren Teilen Nord- und Südamerikas als zuvor an die Ressource in dieser Region weitergeleitet, und mehr Verkehr wird zu Ressourcen in den angrenzenden Regionen 2, 3 und 4 geleitet.



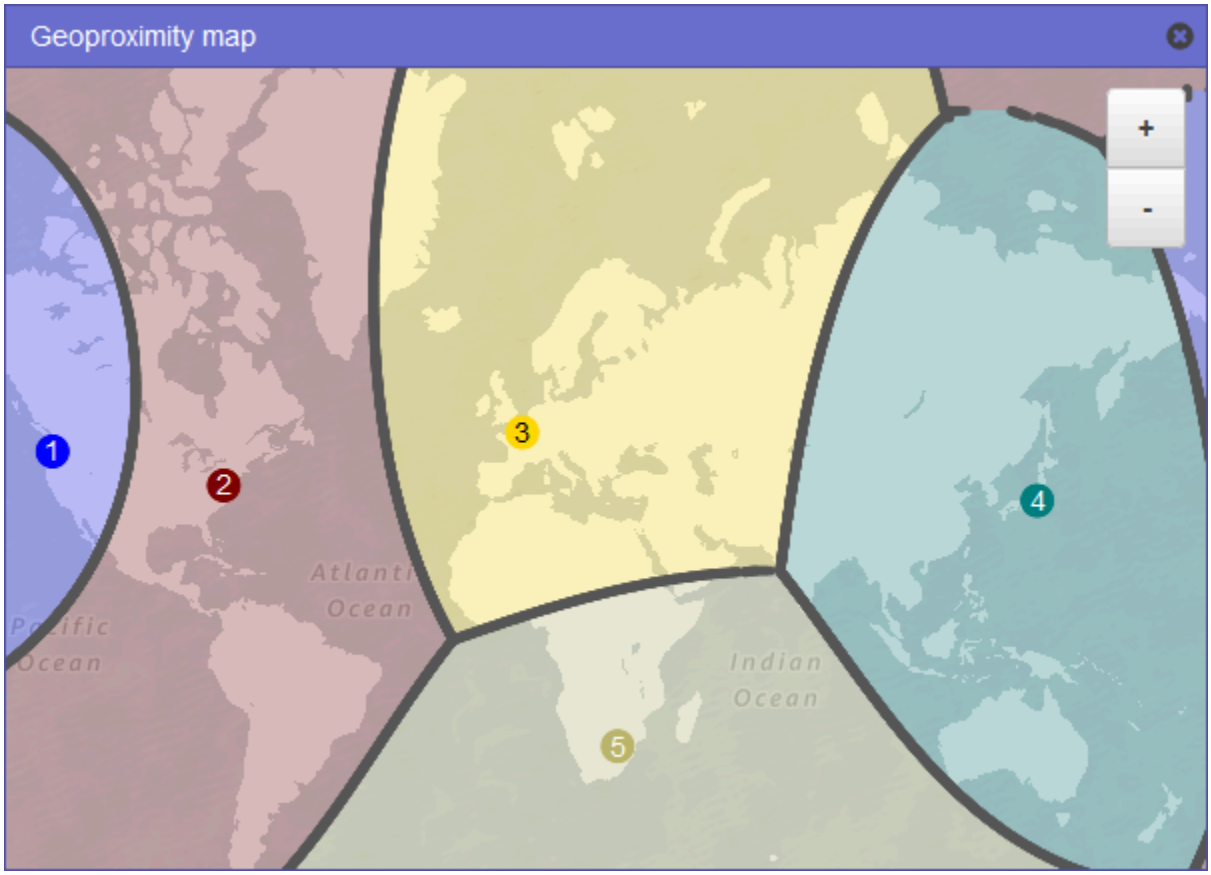
Old console

Die folgende Karte zeigt vier AWS-Regionen (nummeriert von 1 bis 4) und einen Ort in Johannesburg, Südafrika, der nach Breiten- und Längengrad (5) spezifiziert ist.

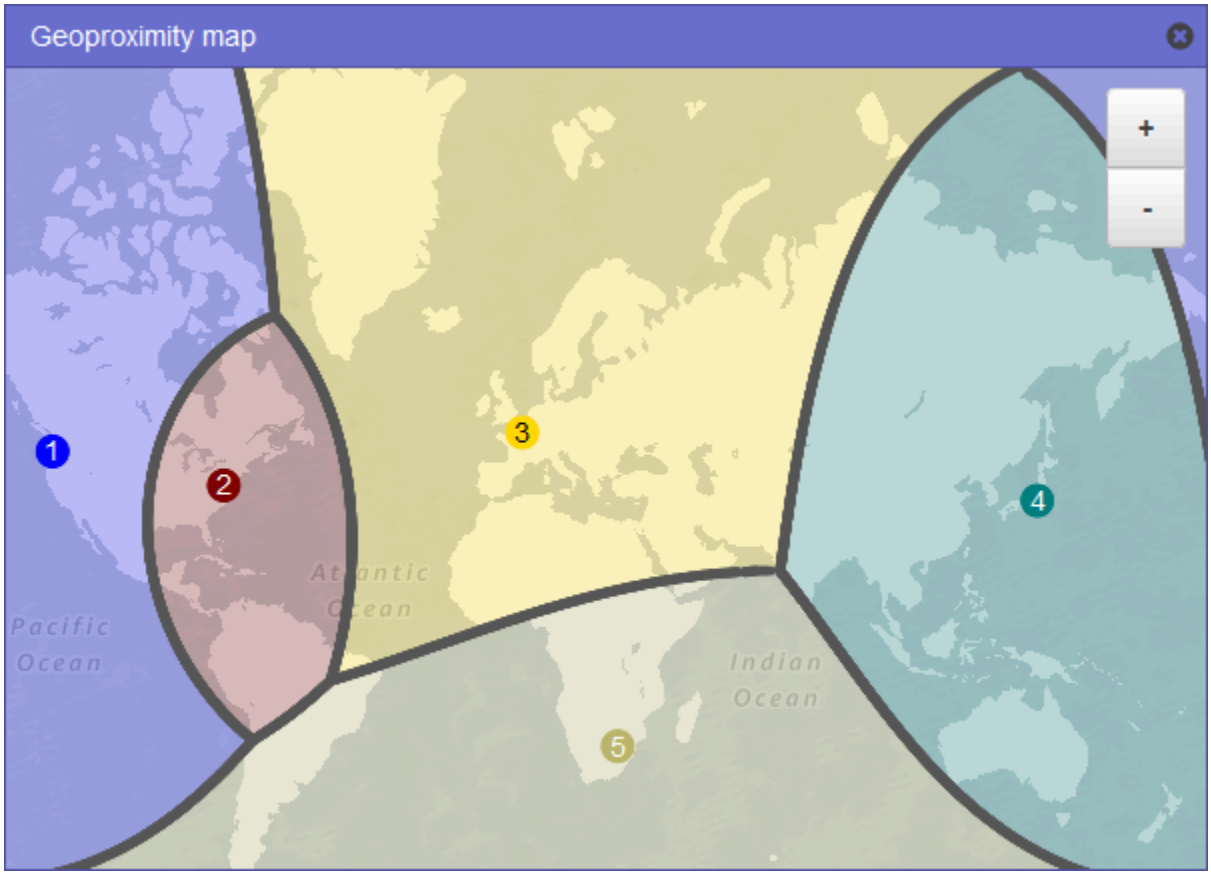
> **Note**
>
> Die Karten sind nur mit Traffic Flow verfügbar.



Die folgende Karte zeigt, was passiert, wenn Sie einen Bias-Wert von +25 für die Region USA Ost (Nord-Virginia) (2 auf der Karte) hinzufügen. Der Datenverkehr wird an die Ressource in dieser Region aus einem größeren Teil Nordamerikas als zuvor und aus ganz Südamerika weitergeleitet.



Die folgende Karte zeigt, was passiert, wenn Sie einen Bias-Wert von -25 für die Region USA Ost (Nord-Virginia) hinzufügen. Der Datenverkehr wird an die Ressource in dieser Region aus kleineren Teilen Nord- und Südamerikas als zuvor weitergeleitet und mehr Datenverkehr an Ressourcen in den angrenzenden Regionen 1, 3 und 5.



Die Auswirkungen der Änderung des Bias-Werts für Ihre Ressourcen ist von einer Reihe von Faktoren abhängig, einschließlich der folgenden:

- Die Anzahl der Ressourcen, die Sie besitzen.
- Die Nähe der Ressourcen zueinander.
- Die Anzahl der Benutzer, die Sie in der Nähe des Grenzbereichs zwischen geografischen Regionen besitzen. Angenommen, Sie haben Ressourcen in den AWS-Regionen USA Ost (Nord-Virginia) und USA West (Oregon) und Sie haben viele Benutzer in Dallas, Austin und San Antonio, Texas, USA. Diese Städte sind ungefähr gleich weit von Ihren Ressourcen entfernt, sodass eine kleine Änderung der Ausrichtung zu einer starken Verlagerung des Datenverkehrs von Ressourcen zwischen Ressourcen führen kann. AWS-Region

Es wird empfohlen, den Bias-Wert in kleinen Schritten zu ändern, um eine Überlastung Ihrer Ressourcen aufgrund einer unerwarteten Verlagerung des Datenverkehrs zu vermeiden.

Weitere Informationen finden Sie unter Wie Amazon Route 53 EDNS0 zur Schätzung des Standorts eines Benutzers nutzt.

So verwendet Amazon Route 53 Bias-Werte

Mit folgender Formel bestimmt Amazon Route 53, wie der Datenverkehr weitergeleitet wird:

Bias

```
Biased distance = actual distance * [1 - (bias/100)]
```

Wenn der Wert der Verzerrung positiv ist, behandelt Route 53 die Quelle einer DNS-Abfrage und die Ressource, die Sie in einem Geoproximitätsdatensatz angeben (z. B. eine EC2 Instanz in einem AWS-Region), so, als ob sie näher beieinander lägen, als sie tatsächlich sind. Angenommen, Sie haben folgende Datensätze der geografischen Nähe:

- Einen Datensatz für Webserver A mit dem positiven Bias-Wert 50
- Einen Datensatz für Webserver B ohne Bias-Wert

Wenn ein Datensatz der geografischen Nähe über den positiven Bias-Wert 50 verfügt, halbiert Route 53 die Entfernung zwischen der Quelle einer Abfrage und der Ressource für diesen Datensatz. Anschließend berechnet Route 53, welche Ressourcen näher an der Quelle der Abfrage liegt. Nehmen wir an, Webserver A ist 150 Kilometer von der Quelle einer Abfrage und Webserver B 100 Kilometer von der Quelle der Abfrage entfernt. Wenn kein Datensatz über einen Bias-Wert verfügt, leitet Route 53 die Abfrage an Webserver B weiter, da dieser näher liegt. Da der Datensatz für Webserver A jedoch über einen positiven Bias-Wert 50 verfügt, behandelt Route 53 Webserver A so, als wäre er 75 Kilometer von der Quelle der Abfrage entfernt. Dies hat zur Folge, dass Route 53 die Abfrage an Webserver A weiterleitet.

Nachfolgend ist die Berechnung für den positiven Bias-Wert 50 aufgeführt:

```
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
```

Latenzbasiertes Routing

Wenn Ihre Anwendung auf mehreren Servern gehostet wird AWS-Regionen, können Sie die Leistung für Ihre Benutzer verbessern, indem Sie ihre Anfragen von dem Server aus bearbeiten AWS-Region , der die niedrigste Latenz bietet.

> **Note**
>
> Die Daten über die Latenz zwischen Benutzern und Ihren Ressourcen basieren ausschließlich auf dem Datenverkehr zwischen Benutzern und AWS -Rechenzentren. Wenn Sie keine Ressourcen in einem verwenden AWS-Region, kann die tatsächliche Latenz zwischen Ihren Benutzern und Ihren Ressourcen erheblich von den AWS Latenzdaten abweichen. Das gilt auch dann, wenn sich Ihre Ressourcen in der gleichen Stadt befinden wie eine AWS-Region.

Um latenzbasiertes Routing zu verwenden, erstellen Sie Latenzdatensätze für Ihre Ressourcen in mehreren AWS-Regionen. Wenn Route 53 eine DNS-Abfrage für Ihre Domain oder Subdomain (example.com oder acme.example.com) erhält, wird ermittelt, für welche AWS-Regionen Sie Latenzdatensätze erstellt haben und welche Region dem Benutzer die niedrigste Latenz bietet. Anschließend wird ein Latenzdatensatz für diese Region ausgewählt. Route 53 antwortet mit dem Wert aus dem ausgewählten Datensatz, z. B. der IP-Adresse für einen Webserver.

Ein Beispiel: Sie verfügen über Elastic Load Balancing Load Balancer in den Regionen USA West (Oregon) und Asien-Pazifik (Singapur). Sie erstellen einen Latenzdatensatz für jeden Load Balancer. Wenn nun ein Benutzer in London den Namen Ihrer Domain in einen Browser eingibt, geschieht Folgendes:

1. DNS leitet die Abfrage an einen Route-53-Namensserver weiter.
2. Route 53 prüft die Latenzdaten zwischen London und der Region Singapur und zwischen London und der Region Oregon.
3. Wenn die Latenz zwischen den Regionen London und Oregon geringer ist, beantwortet Route 53 die Abfrage mit der IP-Adresse für den Oregon-Load Balancer. Wenn die Latenz zwischen den Regionen London und Singapur geringer ist, beantwortet Route 53 die Abfrage mit der IP-Adresse für den Singapur-Load Balancer.

Die Latenz zwischen Hosts im Internet kann sich im Laufe der Zeit ändern. Der Grund dafür sind Veränderungen in puncto Netzwerkkonnektivität und Routing. Latenzbasiertes Routing basiert auf Latenzmessungen, die während eines bestimmten Zeitraums erfasst werden, und die Messungen tragen diesen Änderungen Rechnung. Eine Anforderung, die diese Woche an die Region Oregon weitergeleitet wird, wird nächste Woche möglicherweise an die Region Singapur weitergeleitet.

> **Note**
>
> Wenn ein Browser oder ein anderer Viewer einen DNS-Resolver verwendet, der die edns-client-subnet Erweiterung von EDNS0 unterstützt, sendet der DNS-Resolver an Route 53 eine gekürzte Version der IP-Adresse des Benutzers. Wenn Sie latenzbasiertes Routing konfigurieren, berücksichtigt Route 53 diesen Wert, wenn Datenverkehr zu Ihren Ressourcen weitergeleitet wird. Weitere Informationen finden Sie unter Wie Amazon Route 53 EDNS0 zur Schätzung des Standorts eines Benutzers nutzt.

Sie können Latenz-Routing für Datensätze in einer privat gehosteten Zone verwenden.

Informationen zu Werten, die Sie angeben, wenn Sie die einfache Latenz-Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für Latenz-Datensätze
- Spezifische Werte für Latenz-Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

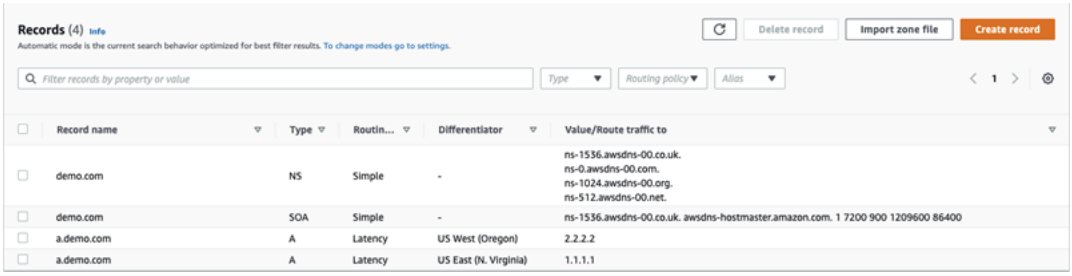
Latenzbasiertes Routing in privat gehosteten Zonen

Für privat gehostete Zonen beantwortet Route 53 DNS-Anfragen mit einem Endpunkt AWS-Region, der sich in derselben oder der nächstgelegenen Entfernung zu AWS-Region der VPC befindet, von der die Anfrage stammt.

> **Note**
>
> Wenn Sie einen ausgehenden Endpunkt an einen eingehenden Endpunkt weitergeleitet haben, wird der Datensatz basierend darauf aufgelöst, wo sich der eingehende Endpunkt befindet, nicht der ausgehende Endpunkt.

Wenn Sie Zustandsprüfungen einbeziehen und der Datensatz mit der niedrigsten Latenz zum Ursprung der Abfrage nicht ordnungsgemäß ist, wird ein fehlerfreier Endpunkt mit der nächstniedrigsten Latenz zurückgegeben.

In der Beispielkonfiguration in der folgenden Abbildung werden DNS-Abfragen, die von einem us-east-1 kommen oder AWS-Region diesem am nächsten liegen, an den 1.1.1.1-Endpunkt weitergeleitet. DNS-Abfragen aus „us-west-2“ oder der nächstgelegenen Region werden an den Endpunkt 2.2.2.2 weitergeleitet.



IP-basiertes Routing

Mit IP-basiertem Routing in Amazon Route 53 können Sie Ihr DNS-Routing feinabstimmen, indem Sie Ihr Verständnis für Ihr Netzwerk, Ihre Anwendungen und Clients nutzen, um die besten DNS-Routing-Entscheidungen für Ihre Endbenutzer zu treffen. IP-basiertes Routing bietet Ihnen eine detaillierte Steuerung zur Optimierung der Leistung oder zur Senkung der Netzwerkkosten, indem Sie Ihre Daten in Form von Zuordnungen auf Route 53 hochladen. user-IP-to-endpoint

Geolokalisierung und latenzbasiertes Routing basieren auf Daten, die Route 53 sammelt und auf dem neuesten Stand hält. Dieser Ansatz funktioniert gut für die Mehrheit der Kunden, aber IP-basiertes Routing bietet Ihnen die zusätzliche Möglichkeit, das Routing basierend auf spezifischen Kenntnissen Ihres Kundenstamms zu optimieren. Beispielsweise möchte ein globaler Anbieter von Videoinhalten möglicherweise Endbenutzer von einem bestimmten Internetdienstanbieter (ISP) weiterleiten.

Nachfolgend finden Sie einige gängige Anwendungsfälle für IP-basiertes Routing:

- Sie möchten Endbenutzer von bestimmten zu bestimmten Endpunkten weiterleiten ISPs , um die Kosten oder die Leistung des Netzwerks zu optimieren.
- Sie möchten bestehenden Route-53-Routing-Typen wie dem Geolocation-Routing basierend auf Ihrem Wissen über die physischen Standorte Ihrer Kunden Außerkraftsetzungen hinzufügen.

IP-Bereiche verwalten und sie einem Ressourcendatensatz zuordnen () RRSet

Für IPv4 können Sie CIDR-Blöcke mit einer Länge von 1 bis einschließlich 24 Bit verwenden, während Sie für IPv6 CIDR-Blöcke mit einer Länge von 1 bis einschließlich 48 Bit verwenden können. Um einen Null-Bit-CIDR-Block (0.0.0.0/0 oder: ::/0) zu definieren, verwenden Sie den Standardstandort („*“).

Bei DNS-Abfragen mit einem CIDR, der länger ist als der in der CIDR-Sammlung angegebene, ordnet Route 53 ihn dem kürzeren CIDR zu. Wenn Sie beispielsweise 2001:0DB8: :/32 als CIDR-Block in Ihrer CIDR-Sammlung angeben und eine Abfrage von DB8 2001:0:0000:1234: :/48 stammt, entspricht sie. Wenn Sie dagegen 2001:0DB8: 0000:1234: :/48 in Ihrer CIDR-Sammlung angeben und eine Abfrage von 2001:0DB8: :/32 stammt, stimmt dies nicht überein und Route 53 antwortet mit dem Datensatz für den Standardstandort („*“).

Sie können Sätze von CIDR-Blöcken (oder IP-Bereichen) in CIDR-Standorten gruppieren, die wiederum in wiederverwendbare Entitäten gruppiert sind, die als CIDR-Sammlungen bezeichnet werden:

CIDR-Block

Ein IP-Bereich in CIDR-Notation, zum Beispiel 192.0.2.0/24 oder 2001:: :/32. DB8

CIDR-Standort

Eine benannte Liste von CIDR-Blöcken. Zum Beispiel example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:: :/32]. DB8 Die Blöcke in einer CIDR-Standortliste müssen nicht benachbart sein oder über denselben Bereich verfügen.

Eine einzelne Position kann sowohl als auch IPv6 Blöcke enthalten, und diese Position kann sowohl A IPv4 - als auch AAAA-Datensätzen zugeordnet werden.

Der Standortname ist gemäß Konvention häufig ein Ort, kann aber auch eine beliebige Zeichenfolge sein (z. B. Unternehmen-A).

CIDR-Sammlung

Eine benannte Sammlung von Standorten. Zum Beispiel mycollection = [example-isp-seattle, example-isp-tokyo].

IP-basierte Routingressourcensätze verweisen auf einen Standort in einer Sammlung, und alle Ressourceneintragssätze für denselben Datensatzsatznamen und -typ müssen auf dieselbe Auflistung verweisen. Wenn Sie beispielsweise Websites in zwei Regionen erstellen und DNS-Abfragen von zwei verschiedenen CIDR-Standorten basierend auf den ursprünglichen IP-

Adressen an eine bestimmte Website leiten möchten, müssen beide Standorte in der gleichen CIDR-Sammlung aufgeführt sein.

Sie können Richtlinien für IP-basiertes Routing nicht für Datensätze in einer privat gehosteten Zone verwenden.

Informationen zu Werten, die Sie angeben, wenn Sie die IP-basierte Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für IP-basierte Datensätze
- Spezifische Werte für IP-basierte Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Themen

- Erstellen einer CIDR-Sammlung mit CIDR-Standorten und -Blöcken
- Arbeiten mit CIDR-Standorten und -Blöcken
- Löschen einer CIDR-Sammlung
- Verschieben einer Geolokalisierung zu IP-basiertem Routing

Erstellen einer CIDR-Sammlung mit CIDR-Standorten und -Blöcken

Erstellen Sie zunächst eine CIDR-Sammlung und fügen Sie CIDR-Blöcke und -Standorte hinzu.

Erstellen Sie eine CIDR-Sammlung mithilfe der Route-53-Konsole wie folgt:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich IP-based routing (IP-basiertes Routing) und dann CIDR collections (CIDR-Sammlungen) aus.
3. Wählen Sie Create CIDR collection (CIDR-Sammlung erstellen) aus.
4. Geben Sie im Bereich Create CIDR collection (CIDR-Sammlung erstellen) unter Details (Details) den Namen für die Sammlung ein.
5. Wählen Sie Create collection (Sammlung erstellen) aus, um eine leere Sammlung zu erstellen.

– oder –

Im Abschnitt CIDR-Standorte erstellen geben Sie im Feld CIDR-Standort einen Namen für den CIDR-Standort ein. Der Standortname kann eine beliebige identifizierende Zeichenfolge sein, z. B. **`company 1`** oder **`Seattle`**. Es muss kein tatsächlicher geografischer Standort sein.

> **Important**
>
> Der CIDR-Standortsname hat eine maximale Länge von 16 Zeichen.

Geben Sie die CIDR-Blöcke in das Feld CIDR-Blöcke ein, einen pro Zeile. Dabei kann es sich IPv4 um IPv6 Adressen im Bereich von /0 bis /24 für IPv4 und /0 bis /48 für handeln. IPv6

6. Nachdem Sie die CIDR-Blöcke eingegeben haben, wählen Sie Create CIDR collection (CIDR-Sammlung erstellen) oder Add another location (Weiteren Standort hinzufügen), um weitere Standorte und CIDR-Blöcke einzugeben. Sie können mehrere CIDR-Standorte pro Sammlung eingeben.
7. Wählen Sie, nachdem Sie CIDR-Standorte eingegeben haben, Create CIDR collection (CIDR-Sammlung erstellen) aus.

Arbeiten mit CIDR-Standorten und -Blöcken

Arbeiten Sie mit CIDR-Standorten über die Route-53-Konsole wie folgt:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im Navigationsbereich IP-based routing (IP-basiertes Routing), CIDR collections (CIDR-Sammlungen) und dann im Bereich CIDR collections (CIDR-Sammlungen) einen Link zu einer CIDR-Sammlung aus der Liste Collection name (Name der Sammlung) aus.

   Auf der Seite CIDR-Standorte können Sie einen CIDR-Standort erstellen, löschen oder einen Standort und seine Blöcke bearbeiten.

   - Um einen Standort zu erstellen, wählen Sie Create CIDR location (CIDR-Standort erstellen) aus.

- Geben Sie im BereichCreate CIDR location (CIDR-Standort erstellen) einen Namen für den Standort und die mit dem Standort verknüpften CIDR-Blöcke ein, und wählen Sie dann Create (Erstellen) aus.
- Um einen CIDR-Standort und die darin enthaltenen Blöcke anzuzeigen, wählen Sie das Optionsfeld neben einem Standort aus, um den Namen und die CIDR-Blöcke im Standortbereich anzuzeigen.

  In diesem Bereich können Sie auch Bearbeiten auswählen, um den Namen des Standorts oder seine CIDR-Blöcke zu aktualisieren. Wählen Sie Save (Speichern) aus, wenn Sie mit der Bearbeitung fertig sind.
- Wählen Sie zum Löschen eines CIDR-Standorts und der darin enthaltenen Blöcke das Optionsfeld neben dem Standort, den Sie löschen möchten, und wählen Sie dann Delete (Löschen) aus. Um den Löschvorgang zu bestätigen, geben Sie den Standortnamen in das Texteingabefeld ein und wählen Sie erneut Delete (Löschen) aus.

  > **Important**
  >
  > Das Löschen eines CIDR-Standorts kann nicht rückgängig gemacht werden. Wenn Sie DNS-Datensätze mit dem Standort verknüpft haben, ist Ihre Domain möglicherweise nicht mehr erreichbar.

Löschen einer CIDR-Sammlung

Löschen Sie eine CIDR-Sammlung, ihre Standorte und Blöcke mithilfe der Route-53-Konsole wie folgt:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich IP-based routing (IP-basiertes Routing) und dann CIDR collections (CIDR-Sammlungen) aus.
3. Klicken Sie im Bereich CIDR collection (CIDR-Sammlung) auf den verknüpften Namen der Sammlung, die Sie löschen möchten.
4. Auf der Seite CIDR locations wählen Sie jeden Standort einzeln aus. Wählen Sie danach Delete (Löschen) aus, geben Sie im Dialogfeld den Namen ein und wählen Sie dann Delete (Löschen)

aus. Sie müssen jeden Standort löschen, der einer CIDR-Auflistung zugeordnet ist, bevor die Sammlung gelöscht werden kann.

5. Nachdem die Löschung jedes CIDR-Standorts abgeschlossen ist, wählen Sie auf der Seite CIDR locations (CIDR-Standorte) das Optionsfeld neben der Sammlung aus, die Sie löschen möchten, und wählen Sie dann Delete (Löschen) aus.

Verschieben einer Geolokalisierung zu IP-basiertem Routing

Wenn Sie entweder Geolokalisierungs- oder Geoproximity-Routing-Richtlinien verwenden und bestimmte Clients konsequent an einen Endpunkt weitergeleitet werden, der basierend auf ihrem physischen Standort oder ihrer Netzwerktopologie nicht optimal ist, können Sie die öffentlichen IP-Bereiche dieser Clients besser mit IP-basiertem Routing ansprechen.

Die folgende Tabelle enthält eine Beispiel-Geolokalisierungskonfiguration für ein vorhandenes Geolokalisierungs-Routing, das wir auf kalifornische IP-Bereiche abstimmen werden.

Datensatzsatzname	Routing-Richtlinie und -Ursprung	IP-Adresse des Anwendung sendpunkts
example.com	Geolocation-Routing (USA)	`198.51.100.1`
example.com	Geolocation-Routing (EU)	`198.51.100.2`

Um IP-Bereiche von Kalifornien zu überschreiben und zu einem neuen Anwendungsendpunkt zu wechseln, erstellen Sie zuerst das Geolokalisierungs-Routing unter einem neuen Datensatznamen neu.

Datensatzname	Routing-Richtlinie und -Ursprung	IP-Adresse des Anwendung sendpunkts
geo.beispiel.com	Geolocation-Routing (USA)	`198.51.100.1`
geo.beispiel.com	Geoloaktion-Routing (EU)	`198.51.100.2`

Erstellen Sie dann IP-basierte Routing-Datensätze und einen Standarddatensatz, der auf Ihren kürzlich neu erstellten Geolocation-Routing-Datensatz verweist.

Datensatzname	Routing-Richtlinie und -Ursprung	IP-Adresse des Anwendungsendpunkts
example.com	IP-basiertes Routing (Standard)	Alias-Datensatz für geo.example.com-Anwendungsendpunkt, den Sie als Standard festlegen möchten Beispiel, `198.51.100.1` .
example.com	IP-basiertes Routing (kalifornische IP-Bereiche)	`198.51.100.3`

Mehrwertiges Antwort-Routing

Bei mehrwertigem Antwort-Routing können Sie Amazon Route 53 so konfigurieren, dass mehrere Werte als Antwort auf DNS-Abfragen zurückgegeben werden, beispielsweise IP-Adressen für Ihre Webserver. Sie können mehrere Werte für nahezu jeden Datensatz festlegen, doch das mehrwertige Antwort-Routing ermöglicht es Ihnen auch, den Zustand jeder Ressource zu überprüfen, sodass Route 53 nur Werte für fehlerfreie Ressourcen zurückgibt. Dies ist kein Ersatz für einen Load Balancer, doch die Möglichkeit, mehrere IP-Adressen mit überprüfbarem Zustand zurückzugeben, ist eine Möglichkeit, DNS zur Verbesserung der Verfügbarkeit und des Lastenausgleichs zu verwenden.

Um Datenverkehr praktisch zufällig zu mehreren Ressourcen weiterzuleiten, beispielsweise Webserver, erstellen Sie einen mehrwertigen Antwortdatensatz für jede Ressource und ordnen optional jedem Datensatz eine Route-53-Zustandsprüfung zu. Route 53 beantwortet DNS-Abfragen mit bis zu acht fehlerfreien Datensätzen und gibt verschiedenen DNS-Resolvern verschiedene Antworten. Wenn ein Webserver nicht mehr verfügbar ist, nachdem ein Resolver eine Antwort im Cache speichert, kann die Client-Software eine andere IP-Adresse in der Antwort ausprobieren.

Beachten Sie Folgendes:

- Wenn Sie einem mehrwertigen Antwortdatensatz eine Zustandsprüfung zuordnen, beantwortet Route 53 DNS-Abfragen nur dann mit der entsprechenden IP-Adresse, wenn die Zustandsprüfung ein fehlerfreies Ergebnis liefert.
- Wenn Sie einen Health Check nicht mit einem mehrwertigen Antwortdatensatz verknüpfen, betrachtet Route 53 den Datensatz immer als fehlerfrei.
- Wenn Sie über acht oder weniger fehlerfreie Datensätze verfügen, beantwortet Route 53 alle DNS-Abfragen mit allen fehlerfreien Datensätzen.
- Wenn alle Datensätze fehlerhaft sind, beantwortet Route 53 DNS-Abfragen mit bis zu acht fehlerhaften Datensätzen.

Sie können mehrwertiges Antwort-Routing für Datensätze in einer privat gehosteten Zone verwenden.

Informationen zu den Werten, die Sie angeben, wenn Sie die Routing-Richtlinie von mehrwertigen Antworten zum Erstellen von Datensätzen verwenden, finden Sie unter Werte für spezifische mehrwertige Antwort-Datensätze und Typische Werte für alle Routing-Richtlinien.

Gewichtetes Routing

Beim gewichteten Routing können Sie mehrere Ressourcen einem einzelnen Domainnamen (example.com) oder Subdomainnamen (acme.example.com) zuordnen und auswählen, wieviel Datenverkehr zu jeder Ressource geleitet wird. Dies kann für verschiedene Zwecke nützlich sein, beispielsweise für den Lastenausgleich und das Testen neuer Softwareversionen.

Um gewichtetes Routing zu konfigurieren, müssen Sie Datensätze mit demselben Namen und Typ für jede Ihrer Ressourcen erstellen. Sie ordnen jedem Datensatz eine relative Gewichtung zu, die dem Volumen an Datenverkehr entspricht, das Sie jeder Ressource senden möchten. Amazon Route 53 sendet Datenverkehr auf Basis der Gewichtung, die Sie einem Datensatz zugeordnet haben, an eine Ressource. Diese Gewichtung stellt einen Anteil der Gesamtgewichtung für alle Datensätze in der Gruppe dar:

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Wenn Sie beispielsweise einen sehr kleinen Teil Ihres Datenverkehrs an eine Ressource senden möchten und den Rest an eine andere Ressource, können Sie Gewichtungen von 1 und 255 angeben. Die Ressource mit der Gewichtung 1 erhält 1/256 des Datenverkehrs (1/1+255) und die andere Ressource erhält 255/256 des Datenverkehrs (255/1+255). Sie können die Waage

schrittweise ändern, indem Sie die Gewichte ändern. Wenn Sie keinen Datenverkehr mehr an eine Ressource senden möchten, können Sie die Gewichtung für diesen Datensatz auf 0 setzen.

Informationen zu Werten, die Sie angeben, wenn Sie die einfache gewichtete Routingrichtlinie zum Erstellen von Datensätzen verwenden, finden Sie in den folgenden Themen:

- Spezifische Werte für gewichtete Datensätze
- Spezifische Werte für gewichtete Aliasdatensätze
- Typische Werte für alle Routing-Richtlinien
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Sie können gewichtetes Routing für Datensätze in einer privat gehosteten Zone verwenden.

Zustandsprüfungen und gewichtetes Routing

Wenn Sie Zustandsprüfungen für alle Datensätze in einer Gruppe von gewichteten Datensätzen hinzufügen, Sie einigen Datensätze jedoch Gewichtungen ungleich Null und anderen Gewichtungen gleich Null geben, funktionieren Zustandsprüfungen ebenso, als ob alle Datensätze Gewichtungen ungleich Null hätten, mit den folgenden Ausnahmen:

- Route 53 berücksichtigt zu Beginn nur die mit nicht-null gewichteten Datensätze, wenn vorhanden.
- Wenn alle Datensätze mit einer Gewichtung größer als 0 fehlerhaft sind, berücksichtigt Route 53 die mit Null gewichteten Datensätze.

In der folgenden Tabelle erfahren Sie, was passiert, wenn der mit Null gewichtete Datensatz eine Zustandsprüfung beinhaltet:

	Datensatz 1	Datensatz 2	Datensatz 3
Gewicht	1	1	0
Zustandsprüfung enthalten?	Ja	Ja	Ja
	Fehlerhaft	Fehlerhaft	Fehlerfrei

	Datensatz 1	Datensatz 2	Datensatz 3
Status der Zustandsprüfung			
DNS-Abfrage beantwortet?	Nein	Nein	Ja
Status der Zustandsprüfung	Fehlerhaft	Fehlerhaft	Fehlerhaft
DNS-Abfrage beantwortet?	Ja	Ja	Nein
Status der Zustandsprüfung	Fehlerhaft	Fehlerfrei	Fehlerhaft
DNS-Abfrage beantwortet?	Nein	Ja	Nein
Status der Zustandsprüfung	Fehlerfrei	Fehlerfrei	Fehlerhaft
DNS-Abfrage beantwortet?	Ja	Ja	Nein
Status der Zustandsprüfung	Fehlerfrei	Fehlerfrei	Fehlerfrei
DNS-Abfrage beantwortet?	Ja	Ja	Nein

In der folgenden Tabelle erfahren Sie, was passiert, wenn der mit Null gewichtete Datensatz keine Zustandsprüfung beinhaltet:

	Datensatz 1	Datensatz 2	Datensatz 3
Gewicht	1	1	0
Zustandsprüfung enthalten?	Ja	Ja	Nein
Status der Zustandsprüfung	Fehlerfrei	Fehlerfrei	–
DNS-Abfrage beantwortet?	Ja	Ja	Nein
Status der Zustandsprüfung	Fehlerhaft	Fehlerhaft	–
DNS-Abfrage beantwortet?	Nein	Nein	Ja
Status der Zustandsprüfung	Fehlerhaft	Fehlerfrei	–
DNS-Abfrage beantwortet?	Nein	Ja	Nein

Wie Amazon Route 53 EDNS0 zur Schätzung des Standorts eines Benutzers nutzt

Um die Genauigkeit von Geolokalisierung, Geoproximität, IP-basiertem Routing und Latenz-Routing zu verbessern, unterstützt Amazon Route 53 die edns-client-subnet Erweiterung von EDNS0.

(EDNS0 fügt mehrere optionale Erweiterungen zum DNS-Protokoll hinzu.) Route 53 kann edns-client-subnet nur verwendet werden, wenn DNS-Resolver dies unterstützen:

- Wenn ein Browser oder ein anderer Viewer einen DNS-Resolver verwendet, der dies nicht unterstützt edns-client-subnet, verwendet Route 53 die Quell-IP-Adresse des DNS-Resolvers, um den ungefähren Standort des Benutzers zu ermitteln, und beantwortet Geolocation-Abfragen mit dem DNS-Eintrag für den Standort des Resolvers.
- Wenn ein Browser oder ein anderer Viewer einen DNS-Resolver verwendet, der dies unterstützt edns-client-subnet, sendet der DNS-Resolver an Route 53 eine gekürzte Version der IP-Adresse des Benutzers. Route 53 bestimmt den Standort des Benutzers auf Basis der abgeschnittenen IP-Adresse anstelle der Quell-IP-Adresse des DNS-Resolvers. Das führt in der Regel zu einer präziseren Schätzung des Standorts eines Benutzers. Route 53 beantwortet Geolocation-Abfragen dann mit dem DNS-Datensatz für den Standort des Benutzers.
- EDNS0 gilt nicht für privat gehostete Zonen. Für privat gehostete Zonen verwendet Route 53 Daten von den VPC-Resolvern, in denen sich AWS-Region die private gehostete Zone befindet, um Entscheidungen über Geolokalisierung und Latenzrouting zu treffen.

Weitere Informationen zu finden Sie im EDNS-Client-Subnetz-RFC edns-client-subnet, Client-Subnetz in DNS-Anfragen.

Wählen zwischen Alias- und Nicht-Alias-Datensätzen

Amazon-Route-53-Aliasdatensätze bieten eine Route-53-spezifische Erweiterung der DNS-Funktionalität. Mit Alias-Datensätzen können Sie Traffic an ausgewählte AWS Ressourcen weiterleiten, einschließlich, aber nicht beschränkt auf CloudFront Distributionen und Amazon S3 S3-Buckets. Außerdem können Sie Datenverkehr von einem Datensatz in einer gehosteten Zone an einen anderen Datensatz weiterleiten.

Im Gegensatz zu einem CNAME-Datensatz können Sie einen Aliasdatensatz am obersten Knoten eines DNS-Namespace erstellen, auch bekannt als Zone Apex. Wenn Sie beispielsweise den DNS-Namen example.com registriert haben, lautet der Zone Apex example.com. Sie können keinen CNAME-Datensatz für example.com erstellen, aber Sie können einen Alias-Datensatz für example.com erstellen, der den Datenverkehr an www.example.com weiterleitet (solange www.example.com nicht des Typs CNAME ist).

Wenn Route 53 eine DNS-Abfrage für einen Alias-Datensatz erhält, beantwortet Route 53 sie mit dem entsprechenden Wert für diese Ressource:

- Eine Amazon-API-Gateway benutzerdefinierte regionale API oder Edge-optimierte API – Route 53 antwortet mit einer oder mehreren IP-Adressen für Ihre API.
- Ein Amazon-VPC-Schnittstellendpunkt – Route 53 antwortet mit einer oder mehreren IP-Adressen für Ihren Schnittstellenendpunkt.
- Eine CloudFront Verteilung — Route 53 antwortet mit einer oder mehreren IP-Adressen für CloudFront Edge-Server, die Ihre Inhalte bereitstellen können.
- App Runner-Dienst — Route 53 antwortet mit einer oder mehreren IP-Adressen.
- Eine Elastic-Beanstalk-Umgebung – Route 53 antwortet mit einer oder mehreren IP-Adressen für die Umgebung.
- Ein Elastic Load Balancing Load Balancer: Route 53 antwortet mit einer oder mehreren IP-Adressen für den Load Balancer. Dazu gehören Application Load Balancer, Classic Load Balancer und Network Load Balancer.
- Ein AWS Global Accelerator Beschleuniger — Route 53 antwortet mit den IP-Adressen für den Beschleuniger.
- Ein OpenSearch Dienst — Route 53 antwortet mit einer oder mehreren IP-Adressen für die benutzerdefinierte OpenSearch Dienstdomäne.
- Ein Amazon-S3-Bucket, das als statische Website konfiguriert ist – Route 53 antwortet mit einer IP-Adresse für den Amazon-S3-Bucket.
- Ein anderer Route-53-Datensatz desselben Typs in derselbenen gehosteten Zone – Route 53 antwortet, als ob die Abfrage nach dem Datensatz gefragt hätte, auf den der Alias-Datensatz verweist (siehe Vergleich von Alias- und CNAME-Datensätzen).
- AWS AppSync Domainname — Route 53 antwortet mit einer oder mehreren IP-Adressen für Ihren Schnittstellenendpunkt.

Weitere Informationen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Wenn Sie einen Aliaseintrag verwenden, um den Verkehr an eine AWS Ressource weiterzuleiten, erkennt Route 53 automatisch Änderungen an der Ressource. Angenommen, ein Alias-Datensatz für example.com verweist auf einen Elastic Load Balancing Load Balancer unter „lb1-1234.us-east-2.elb.amazonaws.com“. Wenn sich die IP-Adresse des Load Balancers ändert, beginnt Route 53 automatisch, DNS-Abfragen unter Verwendung der neuen IP-Adresse zu beantworten.

Wenn ein Aliaseintrag auf eine AWS Ressource verweist, können Sie die Gültigkeitsdauer (Time to Live, TTL) nicht festlegen. Route 53 verwendet die Standard-TTL für die Ressource. Wenn ein

Alias-Datensatz auf einen anderen Datensatz in derselben gehosteten Zone verweist, verwendet Route 53 die TTL des Datensatzes, auf den der Alias-Datensatz verweist. Weitere Informationen zum aktuellen TTL-Wert für Elastic Load Balancing finden Sie unter Anforderungs-Routing im Elastic-Load-Balancing-Benutzerhandbuch und suchen Sie nach „ttl“.

Informationen zur Erstellung von Datensätzen mit der Route-53-Konsole finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole. Informationen über die Werte, die Sie für Alias-Datensätze festlegen, finden Sie unter dem entsprechenden Thema in Werte, die Sie beim Erstellen oder Bearbeiten von Amazon Route 53-Datensätzen angeben:

- Spezifische Werte für einfache Aliasdatensätze
- Spezifische Werte für gewichtete Aliasdatensätze
- Spezifische Werte für Latenz-Aliasdatensätze
- Spezifische Werte für Failover-Aliasdatensätze
- Spezifische Werte für Geolocation-Aliasdatensätze
- Spezifische Werte für Geoproximitäts-Aliasdatensätze
- Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Vergleich von Alias- und CNAME-Datensätzen

Alias-Datensätze ähneln CNAME-Datensätzen. Es gibt jedoch einige wichtige Unterschiede. Die folgende Liste vergleicht Alias- und CNAME-Datensätze.

Ressourcen, an die Sie Abfragen umleiten können

Alias-Datensätze

Ein Aliaseintrag kann Abfragen nur an ausgewählte AWS Ressourcen weiterleiten, einschließlich, aber nicht beschränkt auf die folgenden:

- Amazon-S3-Buckets
- CloudFront Verteilungen
- Ein weiterer Datensatz in derselben gehosteten Route-53-Zone

Beispielsweise können Sie einen Alias-Datensatz mit dem Namen acme.example.com erstellen, der Abfragen an einen Amazon-S3-Bucket mit dem Namen acme.example.com weiterleitet. Sie können auch einen Alias-Datensatz acme.example.com erstellen, der

Abfragen an einen Datensatz mit dem Namen zenith.example.com in der gehosteten Zone "example.com" weiterleitet.

CNAME-Datensätze

Ein CNAME-Datensatz kann DNS-Abfragen an einen beliebigen DNS-Datensatz weiterleiten. Sie können beispielsweise einen CNAME-Datensatz erstellen, der Abfragen von acme.example.com zu zenith.example.com bzw. zu acme.example.org weiterleitet. Sie müssen Route 53 nicht als DNS-Service für die Domain verwenden, an die Sie Abfragen weiterleiten.

Erstellen von Datensätzen mit demselben Namen wie die Domain (Datensätze am Zone Apex)

Alias-Datensätze

In den meisten Konfigurationen können Sie einen Alias-Datensatz erstellen, der denselben Namen wie die gehostete Zone hat (die Zone Apex). Die einzige Ausnahme ist, wenn Sie Abfragen aus der Zone Apex (z. B. example.com) an einen Datensatz in der gleichen gehosteten Zone weiterleiten, die einen Typ CNAME hat (z. B. zenith.example.com). Der Typ des Alias-Datensatzes muss mit dem Typ des Datensatzes übereinstimmen, zu dem Sie Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zone Apex auch für einen Alias-Datensatz nicht unterstützt wird.

CNAME-Datensätze

Es ist nicht möglich, einen CNAME-Datensatz zu erstellen, der denselben Namen wie die gehostete Zone (den Zone Apex) hat. Dies gilt sowohl für gehostete Zonen für Domainnamen (example.com) als auch für gehostete Zonen für Subdomains (zenith.example.com).

Preise für DNS-Abfragen

Alias-Datensätze

Route 53 erhebt keine Gebühren für Aliasabfragen an AWS Ressourcen. Weitere Informationen dazu finden Sie unter Amazon Route 53 – Preise.

CNAME-Datensätze

Route 53 berechnet Gebühren für CNAME-Abfragen.

> **Note**
>
> Wenn Sie einen CNAME-Datensatz erstellen, der an den Namen eines anderen Datensatzes in einer gehosteten Route-53-Zone (dieselbe gehostete Zone oder eine andere gehostete Zone) umleitet, wird jede DNS-Abfrage als zwei Abfragen berechnet:

- Route 53 antwortet auf die erste DNS-Abfrage mit dem Namen des Datensatzes, an den Sie umleiten möchten.
- Dann muss der DNS-Resolver eine weitere Abfrage für den Datensatz in der ersten Antwort senden, um Informationen darüber zu erhalten, wohin der Datenverkehr umgeleitet werden soll, z. B. die IP-Adresse eines Webservers.

Wenn der CNAME-Datensatz an den Namen eines Datensatzes umgeleitet wird, der mit einem anderen DNS-Dienst gehostet wird, berechnet Route 53 eine Abfrage. Der andere DNS-Dienst stellt möglicherweise die zweite Abfrage in Rechnung.

In der DNS-Abfrage angegebener Datensatztyp

Alias-Datensätze

Route 53 antwortet auf eine DNS-Abfrage nur dann, wenn der Name des Alias-Datensatzes (z. B. acme.example.com) und der Typ des Alias-Datensatzes (z. B. A oder AAAA) mit dem Namen und Typ in der DNS-Abfrage übereinstimmt.

CNAME-Datensätze

Ein CNAME-Datensatz leitet DNS-Abfragen für einen Datensatznamen unabhängig von dem in der DNS-Abfrage angegebenen Datensatztyp (z. B. A oder AAAA) um.

Wie Datensätze in dig oder nslookup Abfragen aufgelistet werden

Alias-Datensätze

In der Antwort auf eine dig- oder nslookup-Abfrage wird ein Aliasdatensatz als der beim Erstellen des Datensatzes angegeben Datensatztyp aufgeführt, z. B. A oder AAAA. (Der Datensatztyp, den Sie für einen Alias-Datensatz angeben, hängt von der Ressource ab, an die Sie den Datenverkehr weiterleiten. Um Datenverkehr beispielsweise an einen S3 Bucket weiterzuleiten, geben Sie A als Typ an.) Die Alias-Eigenschaft ist nur in der Route 53-Konsole oder in der Antwort auf eine programmatische Anfrage, z. B. einen AWS `list-resource-record-sets` CLI-Befehl, sichtbar.

CNAME-Datensätze

Ein CNAME-Datensatz wird als CNAME-Datensatz in der Antwort auf dig- oder nslookup-Abfragen aufgeführt.

Unterstützte DNS-Datensatztypen

Amazon Route 53 unterstützt die in diesem Abschnitt aufgelisteten DNS-Datensatztypen. Jeder Datensatztyp umfasst außerdem ein Beispiel dafür, wie das `Value`-Element formatiert wird, wenn Sie auf Route 53 mithilfe der API zugreifen.

> **Note**
>
> Geben Sie für Datensatztypen, die einen Domänennamen enthalten, einen vollständig qualifizierten Domänennamen ein, beispielsweise www.example.com. Der Punkt am Ende ist optional. Route 53 nimmt an, dass der Domänenname vollständig qualifiziert ist. Das bedeutet, dass www.example.com (ohne Punkt am Ende) und www.example.com. (mit Punkt am Ende) von Route 53 identisch gehandhabt werden.

Route 53 bietet eine Erweiterung der DNS-Funktionalität, die als Alias-Datensätze bezeichnet wird. Ähnlich wie bei CNAME-Einträgen können Sie mit Alias-Datensätzen Traffic an ausgewählte AWS Ressourcen wie CloudFront Distributionen und Amazon S3 S3-Buckets weiterleiten. Weitere Hinweise, einschließlich eines Vergleichs von Alias- und CNAME-Datensätzen, finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

- SRV-Datensatztyp
- Typ des SSHFP-Eintrags
- SVCB-Eintragstyp
- TLSA-Eintragstyp
- TXT-Datensatztyp

A-Datensatztyp

Sie verwenden einen A-Eintrag, um den Datenverkehr mithilfe einer IPv4 Adresse in punktierter Dezimalschreibweise an eine Ressource, z. B. einen Webserver, weiterzuleiten.

Beispiel für die Amazon-Route-53-Konsole

```
192.0.2.1
```

Beispiel für die Route-53-API

```
<Value>192.0.2.1</Value>
```

AAAA-Datensatztyp

Sie verwenden einen AAAA-Eintrag, um den Datenverkehr mithilfe einer IPv6 Adresse im durch Doppelpunkte getrennten Hexadezimalformat an eine Ressource, z. B. einen Webserver, weiterzuleiten.

Beispiel für die Amazon-Route-53-Konsole

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Beispiel für die Route-53-API

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA-Datensatztyp

Ein CAA-Eintrag gibt an, welche Zertifizierungsstellen (CAs) Zertifikate für eine Domain oder Subdomain ausstellen dürfen. Durch die Erstellung eines CAA-Eintrags können Sie verhindern, dass

falsche Personen Zertifikate für CAs Ihre Domains ausstellen. Ein CAA Datensatz ist kein Ersatz für die Sicherheitsanforderungen, die von Ihrer Zertifizierungsstelle angegeben werden, beispielsweise die Notwendigkeit, zu bestätigen, dass Sie der Besitzer einer Domäne sind.

Sie können mit CAA-Datensätzen Folgendes angeben:

- Welche Zertifizierungsstellen (CAs) können gegebenenfalls SSL/TLS Zertifikate ausstellen
- Die E-Mail-Adresse oder URL, die zu kontaktieren ist, wenn eine CA ein Zertifikat für die Domäne oder Subdomäne ausstellt.

Wenn Sie Ihrer gehosteten Zone einen CAA-Datensatz hinzufügen, geben Sie drei durch Leerzeichen getrennte Einstellungen an:

```
flags tag "value"
```

Beachten Sie im Hinblick auf das Format der CAA-Datensätze Folgendes:

- Der Wert von `tag` darf nur alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten.
- Schließen Sie `value` in Anführungszeichen ("") ein.
- Einige CAs erlauben oder erfordern zusätzliche Werte für`value`. Geben Sie zusätzliche Werte als Name-Wert-Paare an und trennen Sie sie durch Semikolons (;), z. B.:

  ```
  0 issue "ca.example.net; account=123456"
  ```
- Wenn eine Zertifizierungsstelle eine Anforderung für ein Zertifikat für eine Subdomäne (z. B. www.example.com) erhält und kein CAA-Datensatz für die Subdomäne vorhanden ist, sendet die Zertifizierungsstelle eine DNS-Abfrage für einen CAA-Datensatz für die übergeordnete Domäne (z. B. example.com). Wenn ein Datensatz für die übergeordnete Domäne vorhanden und die Zertifikatsanforderung gültig ist, stellt die Zertifizierungsstelle das Zertifikat für die Subdomäne aus.
- Es wird empfohlen, sich an Ihre CA zu wenden, um die Werte zu ermitteln, die Sie für einen CAA-Datensatz angeben sollten.
- Es ist nicht möglich, einen CAA-Datensatz und einen CNAME-Datensatz mit demselben Namen zu erstellen, weil es DNS nicht zulässt, denselben Namen für einen CNAME-Datensatz und einen beliebigen anderen Datensatz zu verwenden.

Themen

- Autorisieren einer Zertifizierungsstelle zum Ausstellen eines Zertifikats für eine Domäne oder Subdomäne

- Autorisieren einer Zertifizierungsstelle zum Ausstellen eines Platzhalterzertifikats für eine Domäne oder Subdomäne
- Verhindern des Ausstellens eines Zertifikats für eine Domäne oder eine Subdomäne durch eine Zertifizierungsstelle
- Anfordern, dass eine Zertifizierungsstelle Kontakt mit Ihnen aufnimmt, wenn sie eine ungültige Zertifikatanforderung erhält
- Verwenden einer anderen Einstellung, die von der Zertifizierungsstelle unterstützt wird
- Beispiele

Autorisieren einer Zertifizierungsstelle zum Ausstellen eines Zertifikats für eine Domäne oder Subdomäne

Um eine Zertifizierungsstelle zum Ausstellen eines Zertifikats für eine Domäne oder Subdomäne zu autorisieren, erstellen Sie einen Datensatz mit demselben Namen wie die Domäne oder Subdomäne und geben Sie die folgenden Einstellungen an:

- Flags – `0`
- Tag — `issue`
- value – Der Code für die Zertifizierungsstelle, die Sie zum Ausstellen eines Zertifikats für die Domäne oder Subdomäne autorisieren

Angenommen, Sie möchten ca.example.net autorisieren, ein Zertifikat für example.com auszustellen. Sie erstellen einen CAA-Datensatz für example.com mit den folgenden Einstellungen:

```
0 issue "ca.example.net"
```

Informationen zur Autorisierung AWS Certificate Manager zur Ausstellung eines Zertifikats finden Sie unter Konfigurieren eines CAA-Eintrags im AWS Certificate Manager Benutzerhandbuch.

Autorisieren einer Zertifizierungsstelle zum Ausstellen eines Platzhalterzertifikats für eine Domäne oder Subdomäne

Um eine Zertifizierungsstelle zum Ausstellen eines Platzhalterzertifikats für eine Domäne oder Subdomäne zu autorisieren, erstellen Sie einen Datensatz mit demselben Namen wie die Domäne oder Subdomäne und geben Sie die folgenden Einstellungen an. Ein Platzhalterzertifikat gilt für die Domain oder Unterdomain und alle ihre Unterdomains.

- Flags – `0`
- Tag — `issuewild`
- value – Der Code für die Zertifizierungsstelle, die Sie zum Ausstellen eines Zertifikats für die Domäne oder Subdomäne und die entsprechenden Subdomänen autorisieren

Angenommen, Sie möchten ca.example.net zum Ausstellen eines Platzhalterzertifikats für example.com autorisieren, das für example.com und alle entsprechenden Subdomänen gilt. Sie erstellen einen CAA-Datensatz für example.com mit den folgenden Einstellungen:

```
0 issuewild "ca.example.net"
```

Wenn Sie eine Zertifizierungsstelle zum Ausstellen eines Platzhalterzertifikats für eine Domäne oder Subdomäne autorisieren möchten, erstellen Sie einen Datensatz mit demselben Namen wie die Domäne oder Subdomäne und geben Sie die folgenden Einstellungen an. Ein Platzhalterzertifikat gilt für die Domain oder Unterdomain und alle ihre Unterdomains.

Verhindern des Ausstellens eines Zertifikats für eine Domäne oder eine Subdomäne durch eine Zertifizierungsstelle

Um zu verhindern, dass eine Zertifizierungsstelle ein Zertifikat für eine Domäne oder Subdomäne ausstellt, erstellen Sie einen Datensatz mit demselben Namen wie die Domäne oder Subdomäne und geben Sie die folgenden Einstellungen an.

- Flags – `0`
- Etikett — `issue`
- Wert – `";"`

Angenommen, Sie möchten nicht, dass eine Zertifizierungsstelle ein Zertifikat für example.com ausstellt. Sie erstellen einen CAA-Datensatz für example.com mit den folgenden Einstellungen:

```
0 issue ";"
```

Wenn Sie nicht möchten, dass eine Zertifizierungsstelle ein Zertifikat für example.com oder die entsprechenden Subdomänen ausstellt, erstellen Sie einen CAA-Datensatz für example.com mit den folgenden Einstellungen:

```
0 issuewild ";"
```

> **Note**
>
> Wenn Sie einen CAA-Datensatz für example.com erstellen und die folgenden Werte beide angeben, kann eine Zertifizierungsstelle, die den Wert ca.example.net verwendet, das Zertifikat für example.com ausstellen:
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

Anfordern, dass eine Zertifizierungsstelle Kontakt mit Ihnen aufnimmt, wenn sie eine ungültige Zertifikatanforderung erhält

Wenn Sie möchten, dass eine Zertifizierungsstelle, die eine ungültige Anforderung für ein Zertifikat erhält, Kontakt mit Ihnen aufnimmt, geben Sie die folgenden Einstellungen an:

- Flags – `0`
- Etikett — `iodef`
- value – Die URL oder E-Mail-Adresse, die die Zertifizierungsstelle benachrichtigen soll, wenn sie eine ungültige Anforderung für ein Zertifikat erhält Verwenden Sie das entsprechende Format:

  `"mailto:`*`email-address`*`"`

  `"http://`*`URL`*`"`

  `"https://`*`URL`*`"`

Beispiel: Wenn Sie möchten, dass eine Zertifizierungsstelle, die eine ungültige Anforderung für ein Zertifikat erhält, eine E-Mail an admin@example.com sendet, erstellen Sie einen CAA-Datensatz mit den folgenden Einstellungen:

```
0 iodef "mailto:admin@example.com"
```

Verwenden einer anderen Einstellung, die von der Zertifizierungsstelle unterstützt wird

Wenn Ihre Zertifizierungsstelle eine Funktion unterstützt, die nicht gemäß RFC für CAA-Datensätzen definiert ist, geben Sie die folgenden Einstellungen an:

- Flags – 128 (Dieser Wert verhindert, dass die Zertifizierungsstelle ein Zertifikat ausstellt, wenn sie das angegebene Feature nicht unterstützt.)
- Tag – Das Tag, zu dessen Verwendung Sie die Zertifizierungsstelle autorisieren
- value – Der Wert, der dem Wert von „tag“ entspricht

Angenommen, Ihre Zertifizierungsstelle unterstützt das Senden einer Textnachricht, wenn sie eine ungültige Zertifikatanforderung erhält. (Uns sind keine bekannt CAs , die diese Option unterstützen.) Die Einstellungen für den Datensatz können wie folgt lauten:

```
128 exampletag "15555551212"
```

Beispiele

Beispiel für die Route-53-Konsole

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Beispiel für die Route-53-API

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

CNAME-Datensatztyp

Ein CNAME-Datensatz ordnet DNS-Abfragen für den Namen des aktuellen Datensatzes wie „acme.example.com“ einer anderen Domäne („example.com“ oder „example.net“) oder Subdomäne („acme.example.com“ oder „zenith.example.org“) zu.

> **Important**
>
> Das DNS-Protokoll lässt nicht zu, einen CNAME-Datensatz für den obersten Knoten eines DNS-Namespace zu erstellen, auch als Zone Apex bezeichnet. Wenn Sie beispielsweise den DNS-Namen example.com registriert haben, lautet der Zone Apex example.com. Sie können keinen CNAME-Datensatz für example.com erstellen, Sie können jedoch CNAME-Datensätze für www.example.com, newproduct.example.com und so weiter erstellen.

Darüber hinaus gilt: Wenn Sie einen CNAME-Datensatz für eine Subdomäne erstellen, können Sie keine weiteren Datensätze für diese Subdomäne erstellen. Wenn Sie beispielsweise einen CNAME für „www.example.com“ erstellen, können Sie keine weiteren Datensätze erstellen, bei denen der Wert für das Feld Name (Name) „www.example.com“ lautet.

Amazon Route 53 unterstützt auch Alias-Datensätze, mit denen Sie Abfragen an ausgewählte AWS Ressourcen wie CloudFront Distributionen und Amazon S3 S3-Buckets weiterleiten können. Aliasse sind in mancher Hinsicht dem CNAME-Datensatztyp ähnlich; Sie können jedoch einen Alias für den Zone Apex erstellen. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Beispiel für die Route-53-Konsole

```
hostname.example.com
```

Beispiel für die Route-53-API

```
<Value>hostname.example.com</Value>
```

DS-Datensatztyp

Ein Delegierungssignierer-(DS)-Datensatz verweist auf einen Zonenschlüssel für eine delegierte Subdomänenzone. Sie können einen DS-Datensatz erstellen, wenn Sie beim Konfigurieren der DNSSEC-Signatur eine Vertrauenskette einrichten. Weitere Informationen zur Konfiguration von DNSSEC in Route 53 finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

Die ersten drei Werte sind Dezimalzahlen, die den Schlüsseltag, den Algorithmus und den Digesttyp darstellen. Der vierte Wert ist der Digest des Zonenschlüssels. Weitere Informationen zum DS-Datensatz-Format finden Sie unter RFC 4034.

Beispiel für die Route-53-Konsole

```
123 4 5 1234567890abcdef1234567890absdef
```

Beispiel für die Route-53-API

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

HTTPS-Datensatztyp

Ein HTTPS-Ressourceneintrag ist eine Form des Service Binding (SVCB) -DNS-Eintrags, der erweiterte Konfigurationsinformationen bereitstellt, sodass ein Client einfach und sicher eine Verbindung zu einem Dienst über ein HTTP-Protokoll herstellen kann. Die Konfigurationsinformationen werden in Parametern bereitgestellt, die die Verbindung in einer DNS-Abfrage ermöglichen, anstatt dass mehrere DNS-Abfragen erforderlich sind.

Das Format für einen HTTPS-Ressourceneintrag ist:

```
SvcPriority TargetName SvcParams(optional)
```

Die folgenden Parameter werden in RFC 9460, Abschnitt 9.1 beschrieben.

SvcPriority

Eine Ganzzahl, die die Priorität darstellt. Priorität 0 bedeutet Aliasmodus und ist im Allgemeinen für Aliasing am Zonen-Apex vorgesehen. Dieser Wert ist eine Ganzzahl 0-32767 für Route 53, wobei 1-32767 Datensätze im Servicemodus sind. Je niedriger die Priorität, desto höher die Präferenz.

TargetName

Der Domainname entweder des Alias-Ziels (für den Alias-Modus) oder des alternativen Endpunkts (fürServiceMode).

SvcParams (Optional)

Eine durch Leerzeichen getrennte Liste, wobei jeder Parameter aus einem Schlüssel=Wert-Paar oder einem eigenständigen Schlüssel besteht. Wenn es mehr als einen Wert gibt, werden sie als kommagetrennte Liste dargestellt. Die folgenden sind definiert: SvcParams

- `1:alpn`— Protokoll auf Anwendungsebene — Verhandlungsprotokoll IDs. Die Standardeinstellung ist HTTP/1.1, `h2` ist HTTP/2 über TLS und `h3` ist HTTP/3 (HTTP über QUIC-Protokoll).
- `2:no-default-alpn`— Die Standardeinstellung wird nicht unterstützt und Sie müssen einen Parameter angeben. `alpn`
- `3:port`— der alternative Endpunkt oder der Port, über den der Dienst erreicht werden kann.
- `4:ipv4hint`— Hinweise zur IPv4 Adresse.
- `5:ech`— Verschlüsselter Client Hallo.
- `6:ipv6hint`— Hinweise zur IPv6 Adresse.

- `7:dohpath`— DNS-über-HTTPS-Vorlage
- `8:ohttp`— Der Dienst betreibt ein Oblivious-HTTP-Ziel

Beispiel für die Amazon Route 53-Konsole für den Alias-Modus

```
0 example.com
```

Beispiel für die Amazon Route 53-Konsole für den Servicemodus

```
16 example.com alpn="h2,h3" port=808
```

Beispiel für die Amazon Route 53-API für den Alias-Modus

```
<Value>0 example.com</Value>
```

Beispiel für die Route 53-API für den Servicemodus

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Weitere Informationen finden Sie unter RFC 9460, Service Binding and Parameter Specification via DNS (SVCB und HTTPS Resource Records).

> **Note**
>
> Route 53 unterstützt das beliebige Darstellungsformat mit unbekannten Schlüsseln nicht `keyNNNNN`

MX-Datensatztyp

Ein MX-Datensatz gibt die Namen Ihrer Mail-Server und im Fall mehrerer vorhandener Mail-Server die Prioritätsreihenfolge an. Jeder Wert für einen MX-Datensatz enthält zwei Werte, die Priorität und den Domänennamen.

Priorität

Eine Ganzzahl, die die Priorität für einen E-Mail-Server angibt. Wenn Sie nur einen Server angeben, kann die Priorität eine beliebige Zahl zwischen 0 und 65535 sein. Wenn Sie mehrere Server angeben, kennzeichnet der Wert, den Sie für die Priorität angeben, an welchen E-Mail-

Server die E-Mails als Erstes, Zweites usw. geleitet werden sollen. Der Server mit dem niedrigsten Wert für die Priorität erhält den Vorrang. Wenn Sie beispielsweise zwei E-Mail-Server haben und die Werte 10 und 20 für die Priorität angeben, gehen E-Mails immer an den Server mit der Priorität 10, es sei denn, dieser ist nicht verfügbar. Wenn Sie die Werte 10 und 10 angeben, werden E-Mails etwa gleich oft an beide Server geleitet.

Domainname

Der Domänenname des E-Mail-Servers. Geben Sie den Namen (z. B. mail.example.com) eines A- oder AAAA-Datensatzes an. In RFC 2181, Erläuterungen zur DNS-Spezifikation, wird Abschnitt 10.3 verboten, den Namen eines CNAME-Datensatzes für den Domänennamenwert anzugeben. (Wenn im RFC von „Alias" die Rede ist, geht es um einen CNAME-Datensatz, nicht um einen Route-53-Alias-Datensatz.)

Beispiel für die Amazon-Route-53-Konsole

```
10 mail.example.com
```

Beispiel für die Route-53-API

```
<Value>10 mail.example.com</Value>
```

NAPTR-Datensatztyp

Ein Namensvergebungsstellen-Zeiger (NAPTR) ist ein Datensatztyp, der von DDDS-Anwendungen (Dynamic Delegation Discovery System) genutzt wird, um einen Wert in einen anderen zu konvertieren oder einen Wert durch einen anderen zu ersetzen. Eine gängige Anwendung ist beispielsweise die Konvertierung von Telefonnummern in SIP. URIs

Das `Value`-Element für einen NAPTR-Datensatz besteht aus sechs durch Leerzeichen getrennten Werten:

Order

Wenn Sie mehr als einen Datensatz angeben, ist dies die Reihenfolge, in der die DDDS-Anwendung Datensätze auswerten soll. Zulässige Werte: 0 bis 65535.

Präferenz

Wenn Sie zwei oder mehr Datensätze mit derselben Reihenfolge angeben, gibt die Präferenz die Sequenz an, in der die entsprechenden Datensätze ausgewertet werden. Wenn beispielsweise

zwei Datensätze die Reihenfolge 1 haben, wertet die DDDS-Anwendung zuerst den Datensatz mit der niedrigeren Präferenz aus. Zulässige Werte: 0 bis 65535.

Flags

Eine Einstellung speziell für DDDS-Anwendungen. Werte, die derzeit in RFC 3404 definiert sind, sind Groß- und Kleinbuchstaben "A", "P", "S" und "U" sowie eine leere Zeichenfolge "". Schließen Sie Flags in Anführungszeichen ein.

Service

Eine Einstellung speziell für DDDS-Anwendungen. Schließen Sie Service in Anführungszeichen ein.

Weitere Informationen finden Sie in den entsprechenden Dokumenten RFCs:

- URI DDDS-Anwendung — https://tools.ietf.org/html/rfc3404 #section -4.4
- S-NAPTR DDDS-Anwendung — /rfc3958 #section -6.5 https://tools.ietf.org/html
- U-NAPTR DDDS-Anwendung — https://tools.ietf.org/html/rfc4848 #section -4.5

Regexp

Ein regulärer Ausdruck, den die DDDS-Anwendung nutzt, um einen Eingabewert in einen Ausgabewert zu konvertieren. Beispielsweise kann ein IP-Telefonsystem eine regulären Ausdruck verwenden, um eine Telefonnummer, die von einem Benutzer eingegeben wird, in ein SIP-URI umzuwandeln. Schließen Sie Regexp in Anführungszeichen ein. Geben Sie einen Wert für Regexp oder für Ersatz an. Geben Sie aber nicht beide Werte an.

Der reguläre Ausdruck kann folgende druckbaren ASCII-Zeichen enthalten:

- a-z
- 0-9
- - (Bindestrich)
- (Leerzeichen)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (Anführungszeichen). Um ein Anführungszeichen in eine Zeichenfolge einzufügen, stellen Sie ein \-Zeichen voran: \".
- \ (Backslash). Um einen Backslash in eine Zeichenfolge einzufügen, stellen Sie ein \-Zeichen voran: \\.

Geben Sie alle anderen Werte, z. B. internationalisierte Domänennamen, im oktalen Format an.

Die Syntax für Regexp finden Sie in RFC 3402, Abschnitt 3.2, Substitution Expression Syntax

Ersatz

Der vollständig qualifizierte Domänenname (FQDN) des nächsten Domänennamens, an den die DDDS-Anwendung eine DNS-Abfrage senden soll. Die DDDS-Anwendung ersetzt den Eingabewert mit dem von Ihnen angegebenen Wert für Ersatz, falls vorhanden. Geben Sie einen Wert für Regexp oder für Ersatz an. Geben Sie aber nicht beide Werte an. Wenn Sie einen Wert für Regexp angeben, tragen Sie einen Punkt (.) bei Ersatz ein.

Der Domänenname kann a-z, 0-9 und Bindestriche (-) enthalten.

Weitere Informationen zu DDDS-Anwendungen und zu NAPTR-Einträgen finden Sie im Folgenden: RFCs

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Beispiel für die Amazon-Route-53-Konsole

```
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!" .
```

Beispiel für die 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-Datensatztyp

Ein NS-Eintrag identifiziert die Namensserver für die gehostete Zone. Beachten Sie Folgendes:

- Am häufigsten werden NS-Datensätze verwendet, um zu steuern, wie Internetverkehr für eine Domäne weitergeleitet wird. Damit Sie die Datensätze in einer gehosteten Zone zum Weiterleiten von Datenverkehr für eine Domäne verwenden können, aktualisieren Sie die Domänenregistrierungseinstellungen so, dass die vier Nameserver im Standard-NS-Datensatz verwendet werden. (Dies ist der NS-Datensatz, der denselben Namen wie die gehostete Zone hat.)
- Sie können eine separate gehostete Zone für eine Subdomäne (acme.example.com) erstellen und diese gehostete Zone verwenden, um den Internetverkehr für die Subdomäne und deren Subdomänen (subdomain.acme.example.com) weiterzuleiten. Richten Sie diese Konfiguration ein, die bekannt ist als „Delegieren der Zuständigkeit für eine Subdomäne an eine gehostete Zone“, indem Sie einen anderen NS-Datensatz in der gehosteten Zone für die Stammdomäne (example.com) erstellen. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr für Subdomänen.
- NS-Datensätze werden auch verwendet, um White-Label-Name-Server zu konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von White-Label-Nameservern.
- Ein NS-Eintrag kann auch für privat gehostete Zonen verwendet werden, wenn Sie eine Delegiertregel erstellen, um die Autorität für eine Subdomain an Ihren lokalen Resolver zu delegieren. Sie müssen diesen NS-Eintrag erstellen, bevor Sie eine Delegiertenregel erstellen. Weitere Informationen finden Sie unter Wie Resolver-Endpunkte DNS-Anfragen von Ihrem an Ihr Netzwerk weiterleiten VPCs .

Weitere Informationen über NS- und SOA-Einträge finden Sie unter NS- und SOA-Datensätze, die Amazon Route 53 für eine öffentliche gehostete Zone erstellt.

Beispiel für die Amazon-Route-53-Konsole

```
ns-1.example.com
```

Beispiel für die Route-53-API

```
<Value>ns-1.example.com</Value>
```

PTR-Datensatztyp

Ein PTR-Datensatz ordnet eine IP-Adresse dem entsprechenden Domänennamen zu.

Beispiel für die Amazon-Route-53-Konsole

```
hostname.example.com
```

Beispiel für die Route-53-API

```
<Value>hostname.example.com</Value>
```

SOA-Datensatztyp

Ein SOA-Datensatz enthält Informationen zu einer Domäne und der entsprechenden gehosteten Amazon-Route-53-Zone. Weitere Informationen über die einzelnen Felder in einem SOA-Datensatz finden Sie unter NS- und SOA-Datensätze, die Amazon Route 53 für eine öffentliche gehostete Zone erstellt.

Beispiel für die Route-53-Konsole

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Beispiel für die Route-53-API

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF-Datensatztyp

SPF-Datensätze wurden früher verwendet, um die Identität des Absenders von E-Mail-Nachrichten zu überprüfen. Wir empfehlen jedoch nicht mehr, Datensätze mit dem Datensatztyp SPF zu erstellen. RFC 7208, Sender Policy Framework (SPF) für die Autorisierung der Verwendung von Domänen in E-Mail, Version 1, wurde aktualisiert und besagt nun: „... [Seine] Existenz und sein in [RFC4408] definierter Mechanismus haben zu einigen Interoperabilitätsproblemen geführt. Daher ist die Anwendung nicht mehr für SPF-Version 1 geeignet; Implementierungen sollten dies nicht mehr verwenden." Lesen Sie in RFC 7208 Abschnitt 14.1 über SPF DNS-Datensatztypen.

Anstatt einen SPF-Eintrag zu erstellen, empfehlen wir, dass Sie einen TXT-Eintrag mit dem entsprechenden Wert erstellen. Weitere Informationen zu gültigen Werten finden Sie im Wikipedia-Artikel Sender Policy Framework.

Beispiel für die Amazon-Route-53-Konsole

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Beispiel für die Route-53-API

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV-Datensatztyp

Ein `Value`-Element eines SRV-Eintrags besteht aus vier durch Leerzeichen getrennten Werten. Die ersten drei Werte sind Dezimalzahlen, die für Priorität, Gewichtung und den Port stehen. Der vierte Wert ist ein Domänenname. SRV-Einträge werden für den Zugriff auf Services verwendet, z. B. einen Service für E-Mail oder Kommunikation. Weitere Informationen zum SRV-Eintragsformat finden Sie in der Dokumentation des Service, mit dem Sie eine Verbindung herstellen möchten.

Beispiel für die Amazon-Route-53-Konsole

```
10 5 80 hostname.example.com
```

Beispiel für die Route-53-API

```
<Value>10 5 80 hostname.example.com</Value>
```

Typ des SSHFP-Eintrags

Ein Secure Shell-Fingerabdruckeintrag (SSHFP) identifiziert SSH-Schlüssel, die dem Domainnamen zugeordnet sind. SSHFP-Datensätze müssen mit DNSSEC gesichert werden, damit eine Vertrauenskette aufgebaut werden kann. Weitere Informationen zu DNSSEC finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53

Das Format für einen SSHFP-Ressourceneintrag ist:

```
[Key Algorithm] [Hash Type] Fingerprint
```

Die folgenden Parameter sind in RFC 4255 definiert.

Schlüsselalgorithmus

Typ des Algorithmus:

- `0`— Reserviert und nicht verwendet.
- `1: RSA`— Der Rivest-Shamir-Adleman-Algorithmus ist eines der ersten Kryptosysteme mit öffentlichen Schlüsseln und wird immer noch für die sichere Datenübertragung verwendet.

- `2`: `DSA`— Der Algorithmus für digitale Signaturen ist ein Bundesstandard zur Informationsverarbeitung für digitale Signaturen. DSA basiert auf modularer Potenzierung und mathematischen Modellen mit diskretem Logarithmus.
- `3`: `ECDSA`— Der Elliptic Curve Digital Signature Algorithm ist eine Variante des DSA, die Kryptografie mit elliptischen Kurven verwendet.
- `4`: `Ed25519`— Der Ed25519-Algorithmus ist das EdDSA-Signaturschema, das SHA-512 (SHA-2) und Curve25519 verwendet.
- `6`: `Ed448`— Ed448 ist das EddSA-Signaturschema, das Curve448 verwendet. SHAKE256

Hash-Typ

Algorithmus, der zur Erstellung des öffentlichen Schlüssels verwendet wurde:

- `0`— Reserviert und nicht verwendet.
- `1`: `SHA-1`
- `2`: `SHA-256`

Fingerabdruck

Hexadezimale Darstellung des Hashs.

Beispiel für die Amazon-Route-53-Konsole

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Beispiel für die Route-53-API

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

Weitere Informationen finden Sie unter RFC 4255: Verwenden von DNS zur sicheren Veröffentlichung von Secure Shell (SSH) -Schlüsselfingerabdrücken.

SVCB-Eintragstyp

Sie verwenden einen SVCB-Eintrag, um Konfigurationsinformationen für den Zugriff auf Dienstendpunkte bereitzustellen. Der SVCB ist ein generischer DNS-Eintrag und kann verwendet werden, um Parameter für eine Vielzahl von Anwendungsprotokollen auszuhandeln.

Das Format für einen SVCB-Ressourceneintrag ist:

```
SvcPriority TargetName SvcParams(optional)
```

Die folgenden Parameter werden in RFC 9460, Abschnitt 2.3 beschrieben.

SvcPriority

Eine Ganzzahl, die die Priorität darstellt. Priorität 0 steht für Alias-Modus und ist im Allgemeinen für Aliasing am Zonen-Apex vorgesehen. Je niedriger die Priorität, desto höher die Präferenz.

TargetName

Der Domainname entweder des Alias-Ziels (für den Alias-Modus) oder des alternativen Endpunkts (fürServiceMode).

SvcParams (Optional)

Eine durch Leerzeichen getrennte Liste, wobei jeder Parameter aus einem Schlüssel=Wert-Paar oder einem eigenständigen Schlüssel besteht. Wenn es mehr als einen Wert gibt, werden sie als kommagetrennte Liste dargestellt. Dieser Wert ist eine Ganzzahl 0-32767 für Route 53, wobei 1-32767 Datensätze im Servicemodus sind. Die folgenden sind definiert: SvcParams

- `1:alpn`— Protokoll auf Anwendungsebene — Verhandlungsprotokoll IDs. Die Standardeinstellung ist HTTP/1.1, `h2` ist HTTP/2 über TLS und `h3` ist HTTP/3 (HTTP über QUIC-Protokoll).
- `2:no-default-alpn`— Die Standardeinstellung wird nicht unterstützt und Sie müssen einen Parameter angeben. `alpn`
- `3:port`— der Port für den alternativen Endpunkt, über den der Dienst erreicht werden kann.
- `4:ipv4hint`— IPv4 Adressenhinweise.
- `5:ech`— Verschlüsselter Client Hallo.
- `6:ipv6hint`— Hinweise zur IPv6 Adresse.
- `7:dohpath`— DNS-über-HTTPS-Vorlage
- `8:ohttp`— Der Dienst betreibt ein Oblivious-HTTP-Ziel

Beispiel für die Amazon Route 53-Konsole für den Alias-Modus

```
0 example.com
```

Beispiel für die Amazon Route 53-Konsole für den Servicemodus

```
16 example.com alpn="h2,h3" port=808
```

Beispiel für die Amazon Route 53-API für den Alias-Modus

```
<Value>0 example.com</Value>
```

Beispiel für die Route 53-API für den Servicemodus

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Weitere Informationen finden Sie unter RFC 9460, Service Binding and Parameter Specification via DNS (SVCB und HTTPS Resource Records).

> **Note**
>
> Route 53 unterstützt das beliebige Darstellungsformat mit unbekannten Schlüsseln nicht `keyNNNNN`

TLSA-Eintragstyp

Sie verwenden einen TLSA-Datensatz, um die DNS-basierte Authentifizierung benannter Entitäten (DANE) zu verwenden. Ein TLSA-Eintrag ordnet einen certificate/public Schlüssel einem TLS-Endpunkt (Transport Layer Security) zu, und Clients können den certificate/public Schlüssel mithilfe eines mit DNSSEC signierten TLSA-Datensatzes validieren.

TLSA-Einträge können nur als vertrauenswürdig eingestuft werden, wenn DNSSEC in Ihrer Domain aktiviert ist. Weitere Informationen zu DNSSEC finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53

Das Format für einen TLSA-Ressourceneintrag ist:

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

Die folgenden Parameter sind in RFC 6698, Abschnitt 3, spezifiziert.

Verwendung des Zertifikats

Gibt die angegebene Zuordnung an, die für den Abgleich mit dem im TLS-Handshake angegebenen Zertifikat verwendet wird:

- 0: CA Constraint — Das Zertifikat oder der öffentliche Schlüssel muss sich in einem der PKIX-Zertifizierungspfade (Public Key Infrastructure) für das vom Server in TLS bereitgestellte Entity-Zertifikat befinden. Diese Einschränkung schränkt ein, CAs welche Zertifikate für einen bestimmten Dienst ausgestellt werden können.
- 1: Service Certificate Constraint — Gibt ein Endentitätszertifikat (oder den öffentlichen Schlüssel) an, das mit dem vom Server in TLS ausgegebenen Endentitätszertifikat übereinstimmen muss. Diese Zertifizierung schränkt ein, welches Entity-Zertifikat von einem bestimmten Dienst auf einem Host verwendet werden kann.
- 2: Eine Vertrauensanker-Assertion — Gibt ein Zertifikat (oder den öffentlichen Schlüssel) an, das als „Vertrauensanker“ verwendet werden muss, wenn das vom Server in TLS ausgegebene Entity-Zertifikat validiert wird. Ermöglicht einem Domänenadministrator die Angabe eines Vertrauensankers.
- 3: Von einer Domain ausgestellte Zertifizierung — Gibt ein Zertifikat (oder den öffentlichen Schlüssel) an, das mit dem vom Server in TLS ausgestellten Entity-Zertifikat übereinstimmen muss. Diese Zertifizierung ermöglicht es einem Domainadministrator, Zertifikate für eine Domain auszustellen, ohne dass eine Zertifizierungsstelle eines Drittanbieters hinzugezogen werden muss. Dieses Zertifikat muss die PKIX-Validierung nicht bestehen.

Selector

Gibt an, welcher Teil des vom Server im Handshake vorgelegten Zertifikats mit dem Zuordnungswert abgeglichen wird:

- 0: Das gesamte Zertifikat muss abgeglichen werden.
- 1: Der öffentliche Subject-Schlüssel oder die DER-kodierte Binärstruktur müssen übereinstimmen.

Passender Typ

Gibt die Präsentation (wie im Feld Selector festgelegt) des Zertifikatsabgleichs an:

- 0: Exakte Übereinstimmung mit dem Inhalt.
- 1: SHA-256-Hash.
- 2: SHA-512-Hash.

Daten zur Zertifikatsvereinigung

Die abzugleichenden Daten basieren auf den Einstellungen der anderen Felder.

Beispiel für die Amazon-Route-53-Konsole

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Beispiel für die Route-53-API

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

Weitere Informationen finden Sie unter RFC 6698, Das DNS-based Authentication of Named Entities (DANE) Transport Layer Security (TLS) -Protokoll: TLSA.

TXT-Datensatztyp

Ein TXT-Datensatz enthält eine oder mehrere Zeichenfolgen, die in Anführungszeichen eingeschlossen sind (''). Wenn Sie die einfache Routing-Richtlinie verwenden, nehmen Sie alle Werte für eine Domäne (example.com) oder Subdomäne (www.example.com) in den gleichen TXT-Datensatz auf.

Themen

- Eingeben von TXT-Datensatzwerten
- Sonderzeichen in einem TXT-Datensatzwert
- Groß- und Kleinbuchstaben in einem TXT-Datensatzwert
- Beispiele

Eingeben von TXT-Datensatzwerten

Eine einzelne Zeichenfolge kann bis zu 255 Zeichen umfassen, einschließlich der folgenden:

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

Wenn Sie einen Wert eingeben müssen, der länger als 255 Zeichen ist, teilen Sie den Wert in Zeichenfolgen mit höchstens 255 Zeichen auf und schließen Sie jede Zeichenfolge in doppelte Anführungszeichen ein (''). Führen Sie in der Konsole alle Zeichenfolgen in derselben Zeile auf:

```
"String 1" "String 2" "String 3"
```

Fügen Sie für die API alle Zeichenfolgen in demselben `Value`-Element ein:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

Die maximale Länge eines Wertes in einem TXT-Datensatz beträgt 4.000 Zeichen.

Um mehr als einen TXT-Wert einzugeben, geben Sie einen Wert pro Zeile ein.

Sonderzeichen in einem TXT-Datensatzwert

Wenn Ihr TXT-Eintrag eines der folgenden Zeichen enthält, müssen Sie die Zeichen mithilfe von Escape-Codes im folgenden Format angeben: \ *three-digit octal code*

- Zeichen 000 bis 040 oktal (0 bis 32 dezimal, 0x00 bis 0x20 hexadezimal)
- Zeichen 177 bis 377 oktal (127 bis 255 dezimal, 0x7F bis 0xFF hexadezimal)

Wenn der Wert Ihres TXT-Datensatzes z. B. `"exämple.com"` ist, geben Sie `"ex\344mple.com"` an.

Für eine Zuordnung zwischen ASCII-Zeichen und Oktalcodes führen Sie eine Internetsuche nach „ASCII-Oktalcodes“ durch. Eine nützliche Referenz ist ASCII Code - The extended ASCII table.

Um ein Anführungszeichen (") in eine Zeichenfolge aufzunehmen, setzen Sie einen umgekehrten Schrägstrich (\) vor das Anführungszeichen: \".

Groß- und Kleinbuchstaben in einem TXT-Datensatzwert

Die Groß-/Kleinschreibung wird berücksichtigt, sodass `"Ab"` und `"aB"` verschiedene Werte darstellen.

Beispiele

Beispiel für die Amazon-Route-53-Konsole

Geben Sie jeden Wert in einer separaten Zeile ein:

```
"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"
```

Beispiel für die Route-53-API

Geben Sie jeden Wert in einem `Value`-Element ein:

```
<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>
```

Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole

Im folgenden Verfahren wird das Erstellen von Datensätzen mit der Amazon-Route-53-Konsole erläutert. Informationen zum Erstellen von Datensätzen mithilfe der Route 53-API finden Sie ChangeResourceRecordSetsin der Amazon Route 53-API-Referenz.

> **Note**
>
> Um Datensätze für komplexe Routing-Konfigurationen zu erstellen, können Sie auch den visuellen Traffic Flow Editor verwenden und die Konfiguration als Verkehrsrichtlinie speichern. Sie können dann die Datenverkehrsrichtlinie mit einem oder mehreren Domainnamen (z. B. example.com) oder Subdomainnamen (z. B. www.example.com) in derselben gehosteten Zone oder in mehreren gehosteten Zonen verknüpfen. Außerdem können Sie ein Rollback der Aktualisierungen durchführen, wenn die neue Konfiguration sich nicht wie erwartet verhält. Weitere Informationen finden Sie unter Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr.

So erstellen Sie einen Datensatz mit der Route-53-Konsole:

1. Wenn Sie keinen Alias-Datensatz erstellen, fahren Sie mit Schritt 2 fort.

   Fahren Sie auch mit Schritt 2 fort, wenn Sie einen Aliaseintrag erstellen, der DNS-Verkehr an eine andere AWS Ressource als einen Elastic Load Balancing Load Balancer oder einen anderen Route 53-Datensatz weiterleitet.

   Wenn Sie einen Alias-Datensatz erstellen, der Datenverkehr an einen Elastic Load Balancing Load Balancer weiterleitet, und Sie Ihre gehostete Zone und Ihren Load Balancer mit verschiedenen Konten erstellt haben, befolgen Sie die Schritte im Verfahren Abrufen des DNS-

Namens für einen Elastic Load Balancing Load Balancer, um den DNS-Namen für den Load Balancer abzurufen.

2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wenn Sie bereits über eine gehostete Zone für Ihre Domain verfügen, fahren Sie mit Schritt 5 fort. Wenn Sie dies nicht tun, führen Sie die entsprechenden Schritte aus, um eine gehostete Zone zu erstellen:

   - Informationen zur Weiterleitung des Internetverkehrs zu Ihren Ressourcen wie Amazon S3 S3-Buckets oder EC2 Amazon-Instances finden Sie unterErstellen einer öffentlichen gehosteten Zone.
   - Informationen zum Weiterleiten von Datenverkehr in Ihrer VPC finden Sie unter Erstellen einer privat gehosteten Zone.
5. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) den Namen der gehosteten Zone aus, in der Sie Datensätze erstellen möchten.
6. Wählen Sie Create record (Datensatz erstellen).
7. Wählen und definieren Sie die anwendbare Routingrichtlinie und -werte. Weitere Informationen finden Sie im Thema zu der Art des Datensatzes, die Sie erstellen möchten:

   - Typische Werte für alle Routing-Richtlinien
   - Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind
   - Spezifische Werte für einfache Datensätze
   - Spezifische Werte für einfache Aliasdatensätze
   - Spezifische Werte für Failover-Datensätze
   - Spezifische Werte für Failover-Aliasdatensätze
   - Spezifische Werte für Geolocation-Datensätze
   - Spezifische Werte für Geolocation-Aliasdatensätze
   - Spezifische Werte für Geoproximitätsdatensätze
   - Spezifische Werte für Geoproximitäts-Aliasdatensätze
   - Spezifische Werte für Latenz-Datensätze
   - Spezifische Werte für Latenz-Aliasdatensätze
   - Spezifische Werte für IP-basierte Datensätze

- Spezifische Werte für IP-basierte Aliasdatensätze
- Werte für spezifische mehrwertige Antwort-Datensätze
- Spezifische Werte für gewichtete Datensätze
- Spezifische Werte für gewichtete Aliasdatensätze

8. Wählen Sie Create records (Datensätze erstellen).

> **Note**
>
> Die Verteilung Ihrer neuen Datensätze auf die Route-53-DNS-Server nimmt etwas Zeit in Anspruch. Derzeit besteht die einzige Möglichkeit, um zu überprüfen, ob Änderungen übernommen wurden, darin, die GetChangeAPI-Aktion zu verwenden. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

9. Wenn Sie mehrere Datensätze erstellen, wiederholen Sie die Schritte 7 bis 8.

Abrufen des DNS-Namens für einen Elastic Load Balancing Load Balancer

1. Melden Sie sich AWS-Managementkonsole mit dem AWS Konto an, mit dem Sie den Classic-, Application- oder Network Load Balancer erstellt haben, für den Sie einen Aliaseintrag erstellen möchten.
2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Klicken Sie im Navigationsbereich auf Load Balancers.
4. Wählen Sie in der Liste der Load Balancer den Load Balancer aus, für den Sie einen Alias-Datensatz erstellen möchten.
5. Ermitteln Sie auf der Registerkarte Description den Wert bei DNS name.
6. Wiederholen Sie die Schritte 4 und 5, wenn Sie Alias-Datensätze für andere Elastic Load Balancing Load Balancer erstellen möchten.
7. Melden Sie sich von der ab AWS-Managementkonsole.
8. Melden Sie sich AWS-Managementkonsole erneut mit dem AWS Konto an, mit dem Sie die gehostete Route 53-Zone erstellt haben.
9. Gehen Sie zurück zu Schritt 3 des Verfahrens Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

Berechtigungen für Ressourcendatensätze

Berechtigungen für Ressourcendatensätze verwenden die Richtlinienbedingungen für Identity and Access Management (IAM), damit Sie detaillierte Berechtigungen für Aktionen auf der Route 53-Konsole oder für die Verwendung der ChangeResourceRecordSetsAPI festlegen können.

Ein Ressourcendatensatz ist definiert als mehrere Ressourceneinträge mit demselben Namen und Typ (und derselben Klasse, aber für die meisten Zwecke ist die Klasse immer IN oder Internet), die jedoch unterschiedliche Daten enthalten. Wenn Sie beispielsweise Geolocation-Routing wählen, können Sie mehrere A- oder AAAA-Datensätze haben, die auf verschiedene Endpunkte für dieselbe Domain verweisen. Alle diese A- oder AAAA-Datensätze bilden zusammen einen Ressourcendatensatz. Weitere Informationen zur DNS-Terminologie finden Sie unter RFC 7719.

Mit den IAM-Richtlinienbedingungen, `route53:ChangeResourceRecordSetsNormalizedRecordNames` `route53:ChangeResourceRecordSetsRecordTypesroute53:ChangeResourceRecordSetsActio` und können Sie anderen AWS Benutzern in jedem anderen Konto detaillierte Administratorrechte gewähren. AWS Auf diese Weise können Sie jemandem Berechtigungen erteilen für:

- Einen einzelnen Ressourcendatensatz.
- Alle Ressourceneintragssätze eines bestimmten DNS-Eintragstyps.
- Ressourcendatensätze, bei denen die Namen eine bestimmte Zeichenfolge enthalten.
- Führen Sie einige oder alle `CREATE | UPSERT | DELETE` Aktionen aus, wenn Sie die ChangeResourceRecordSetsAPI oder die Route 53-Konsole verwenden.

Sie können auch Zugriffsberechtigungen erstellen, die eine der Route 53-Richtlinienbedingungen kombinieren. Sie können beispielsweise jemandem die Berechtigung erteilen, die A-Datensatzdaten für marketing-example.com zu ändern, diesem Benutzer jedoch nicht erlauben, Datensätze zu löschen.

Weitere Informationen zu Berechtigungen für Ressourcendatensätze und Beispiele für deren Verwendung finden Sie unterVerwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

Informationen zur Authentifizierung von AWS Benutzern finden Sie unterAuthentifizierung mit Identitäten. Informationen zum Steuern des Zugriffs auf Route 53-Ressourcen finden Sie unterZugriffskontrolle.

Werte, die Sie beim Erstellen oder Bearbeiten von Amazon Route 53-Datensätzen angeben

Wenn Sie Datensätze mit der Amazon Route 53-Konsole erstellen, hängen die von Ihnen angegebenen Werte von der Routing-Richtlinie ab, die Sie verwenden möchten, und davon, ob Sie Alias-Datensätze erstellen, die den Verkehr zu AWS Ressourcen weiterleiten.

Alias-Datensätze, die Traffic an bestimmte AWS Ressourcen weiterleiten, für die Sie die Zielressource angeben (z. B. Elastic Load Balancing, CloudFront Distribution, Amazon S3 S3-Bucket). Sie können optional auch Zustandsprüfungen verknüpfen und die Zielzustandsprüfung konfigurieren. Die folgenden Themen enthalten detaillierte Informationen zu den Werten, die für jede Routing-Richtlinie und jeden Datensatztyp erforderlich sind, sodass Sie Ihre Route 53-Datensätze effektiv konfigurieren können.

Themen

Typische Werte für alle Routing-Richtlinien

Das sind die Werte, die Sie bei der Erstellung oder Bearbeitung von Amazon Route 53-Datensätzen angeben. Diese Werte werden von allen Routing-Richtlinien verwendet.

Themen

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

CNAME-Datensätze

Wenn Sie einen Datensatz erstellen, der den Wert CNAME für Datensatztyp hat, darf der Name für den Datensatz nicht gleich dem Namen der gehosteten Zone sein.

Sonderzeichen

Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

Platzhalterzeichen

Sie können im Namen ein Sternchenzeichen (*) verwenden. Abhängig von seiner Position im Namen wird das *-Zeichen vom DNS entweder als Platzhalter oder als das *-Zeichen (ASCII 42) behandelt. Weitere Informationen finden Sie unter Verwendung eines Sternchens (*) im Namen von gehosteten Zonen und Datensätzen.

> **Important**
>
> Sie können den Platzhalter * nicht für Ressourcendatensätze mit dem Typ NS verwenden.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

A — IPv4 Adresse

Eine IP-Adresse im IPv4 Format, zum Beispiel 192.0.2.235.

AAAA — Adresse IPv6

Eine IP-Adresse im IPv6 Format, zum Beispiel 2001:0 db 8:85 a 3:0:0:0:8 a2e: 0370:7334.

CAA – Autorisierung der Zertifizierungsstelle

Drei durch Leerzeichen voneinander getrennte Werte, die festlegen, welche Zertifizierungsstellen Zertifikate oder Platzhalterzertifikate für die in Datensatzname angegebene Domäne oder Subdomäne ausstellen dürfen. Sie können mit CAA-Datensätzen Folgendes angeben:

- Welche Zertifizierungsstellen () können gegebenenfalls SSL/TLS-Zertifikate ausstellen CAs
- Die E-Mail-Adresse oder URL, die zu kontaktieren ist, wenn eine CA ein Zertifikat für die Domäne oder Subdomäne ausstellt.

CNAME – kanonischer Name

Der vollständig qualifizierte Domänenname (zum Beispiel www.example.com), an den Route 53 die Antworten auf DNS-Abfragen für diesen Datensatz zurückgeben soll. Ein abschließender Punkt ist optional. Route 53 nimmt an, dass der Domänenname vollständig qualifiziert ist. Das bedeutet, dass www.example.com (ohne Punkt am Ende) und www.example.com. (mit Punkt am Ende) von Route 53 identisch gehandhabt werden.

MX – Mail-Austausch

Eine Priorität und ein Domänenname, der einen Mail-Server angibt, zum Beispiel 10 mailserver.example.com. Der abschließende Punkt wird als optional behandelt.

NAPTR – Name Authority Pointer (Namensautorisierungszeiger)

Sechs durch Leerzeichen getrennte Einstellungen, die von DDDS-Anwendungen (Dynamic Delegation Discovery System) verwendet werden, um einen Wert in einen anderen zu konvertieren oder einen Wert durch einen anderen zu ersetzen. Weitere Informationen finden Sie unter NAPTR-Datensatztyp.

PTR – Pointer (Zeiger)

Der Domänenname, den Route 53 zurückgeben soll.

NS – Namenserver

Der Domänenname eines Namens-Servers wie ns1.example.com.

> **Note**
>
> Sie können einen NS-Datensatz nur mit einfacher Routing-Richtlinie angeben.

SPF – Sender Policy Framework.

Ein SPF-Datensatz in Anführungszeichen, zum Beispiel "v=spf1 ip4:192.168.0.1/16-all". SPF-Einträge werden nicht empfohlen. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

SRV – Service-Locator

Ein SRV-Eintrag. SRV-Einträge werden für den Zugriff auf Services verwendet, z. B. einen Service für E-Mail oder Kommunikation. Weitere Informationen zum SRV-Eintragsformat finden Sie in der Dokumentation des Service, mit dem Sie eine Verbindung herstellen möchten. Ein abschließender Punkt wird als optional behandelt.

Das Format eines SRV-Eintrags ist folgendermaßen:

[Priorität] [Gewichtung] [Port] [Server-Host-Name]

Beispiel:

1 10 5269 xmpp-server.example.com.

TXT – Text

Ein Texteintrag. Schließen Sie den Text in Anführungszeichen ein, z. B. „Beispieltexteintrag“.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Werte, die für Aliasdatensätze für alle Routing-Richtlinien typisch sind

Das sind die Werte, die Sie bei der Erstellung oder Bearbeitung von Amazon Route 53-Datensätzen angeben. Diese Werte werden von allen Routing-Richtlinien verwendet.

Themen

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

CNAME-Datensätze

Wenn Sie einen Datensatz erstellen, der den Wert CNAME für Type (Typ) hat, darf der Name für den Datensatz nicht gleich dem Namen der gehosteten Zone sein.

Aliase für CloudFront Distributionen und Amazon S3 S3-Buckets

Der Wert, den Sie angeben, hängt zum Teil von der AWS Ressource ab, an die Sie den Datenverkehr weiterleiten:

- CloudFront Verteilung — Ihre Distribution muss einen alternativen Domainnamen enthalten, der dem Namen des Eintrags entspricht. Wenn der Name des Datensatzes beispielsweise acme.example.com ist, muss Ihre CloudFront-Verteilung acme.example.com als einen alternativen Domänennamen enthalten. Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen (CNAMEs) im Amazon CloudFront Developer Guide.
- Amazon-S3-Bucket – Der Name des Datensatzes muss mit dem Namen Ihres Amazon-S3-Buckets übereinstimmen. Wenn der Name des Buckets beispielsweise acme.example.com lautet, muss der Name dieses Datensatzes ebenfalls acme.example.com lauten.

Außerdem müssen Sie den Bucket für das Website-Hosting konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Buckets für Website-Hosting im Benutzerhandbuch für Amazon Simple Storage Service.

Sonderzeichen

Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

Platzhalterzeichen

Sie können im Namen ein Sternchenzeichen (*) verwenden. Abhängig von seiner Position im Namen wird das *-Zeichen vom DNS entweder als Platzhalter oder als das *-Zeichen (ASCII 42) behandelt. Weitere Informationen finden Sie unter Verwendung eines Sternchens (*) im Namen von gehosteten Zonen und Datensätzen.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Datenverkehr weiterleiten.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Verkehr zu bestimmten AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Important

Wenn Sie dasselbe AWS Konto verwendet haben, um Ihre Hosting-Zone und die Ressource zu erstellen, zu der Sie den Datenverkehr weiterleiten, und wenn Ihre Ressource nicht in der Endpunktliste erscheint, überprüfen Sie Folgendes:

- Sie müssen einen unterstützten Wert für Datensatztyp auswählen. Unterstützte Werte sind spezifisch für die Ressource, auf die Sie den Datenverkehr leiten. Um beispielsweise Traffic an einen S3-Bucket weiterzuleiten, müssen Sie A — IPv4 address als Datensatztyp auswählen.
- Das Konto muss über die IAM-Berechtigungen verfügen, die zum Auflisten der entsprechenden Ressourcen erforderlich sind. Damit beispielsweise CloudFront-Verteilungen in der Liste Endpoint (Endpunkt) angezeigt werden, muss das Konto über die Berechtigung zum Ausführen der folgenden Aktion verfügen: `cloudfront:ListDistributions`.

Eine IAM-Beispielrichtlinie finden Sie unter Erforderliche Berechtigungen zur Verwendung der Amazon-Route-53-Konsole.

Wenn Sie verschiedene AWS Konten verwendet haben, um die gehostete Zone und die Ressource zu erstellen, wird Ihre Ressource in der Endpunktliste nicht angezeigt. In der folgenden Dokumentation zu Ihrem Ressourcentyp erfahren Sie, welchen Wert Sie unter Endpunkt eingeben müssen.

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Führen Sie für API Gateway Custom Regional APIs und Edge-Optimized APIs einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihrer API dasselbe Konto verwenden – Wählen Sie Endpunkt und anschließend eine API aus der Liste aus. Wenn Sie viele haben APIs, können Sie die ersten Zeichen des API-Endpunkts eingeben, um die Liste zu filtern.

  > **Note**
  >
  > Der Name dieses Datensatzes muss mit einem benutzerdefinierten Domänennamen für Ihre API übereinstimmen, z. B. api.example.com.

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihrer API verschiedene Konten verwenden – Geben Sie den API-Endpunkt für die API ein, z. B. api.example.com.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen einer API verwendet haben, wird die API nicht in der Liste Endpoints unter API Gateway APIs angezeigt.

  Wenn Sie ein Konto verwendet haben, um die aktuelle Hosting-Zone zu erstellen, und ein oder mehrere verschiedene Konten, um all Ihre Konten zu erstellen APIs, wird in der Liste Endpoints unter API Gateway APIs Keine Ziele verfügbar angezeigt. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens.

CloudFront Distributionen

Führen Sie für CloudFront Verteilungen einen der folgenden Schritte aus:

- Wenn Sie dasselbe Konto verwendet haben, um Ihre Route 53-Hosting-Zone und Ihre CloudFront Distribution zu erstellen, wählen Sie Endpoint und wählen Sie eine Distribution aus der Liste aus. Bei einer großen Anzahl von Verteilungen können Sie die ersten Zeichen des Domänennamens der Verteilung eingeben, um die Liste zu filtern.

  Beachten Sie Folgendes, wenn Ihre Verteilung nicht in der Liste angezeigt wird:

  - Der Name dieses Datensatzes muss mit einem alternativen Domänennamen in Ihrer Verteilung übereinstimmen.
  - Wenn Sie Ihrer Distribution gerade einen alternativen Domainnamen hinzugefügt haben, kann es 15 Minuten dauern, bis Ihre Änderungen an allen CloudFront Edge-Standorten wirksam werden. Erst wenn die Änderungen propagiert wurden, kann Route 53 den neuen alternativen Domänennamen kennen.
- Wenn Sie verschiedene Konten verwendet haben, um Ihre Route 53-Hosting-Zone und Ihre Distribution zu erstellen, geben Sie den CloudFront Domainnamen für die Verteilung ein, z. B. d111111abcdef8.cloudfront.net.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen einer Verteilung verwendet haben, wird die Verteilung nicht in der Liste der Endpoints angezeigt.

  Wenn Sie ein Konto zum Erstellen der aktuellen Hostzone und ein oder mehrere verschiedene Konten zum Erstellen all Ihrer Verteilungen verwendet haben, wird in der Liste Endpunkte unter Verteilungen der Eintrag Keine Ziele verfügbar angezeigt. CloudFront

> **Important**
>
> Leiten Sie Abfragen nicht an eine CloudFront Verteilung weiter, die nicht an allen Edge-Standorten verbreitet wurde, da Ihre Benutzer sonst nicht auf die entsprechenden Inhalte zugreifen können.

Ihre CloudFront Distribution muss einen alternativen Domainnamen enthalten, der dem Namen des Eintrags entspricht. Wenn der Name des Eintrags beispielsweise acme.example.com lautet, muss Ihre CloudFront Distribution acme.example.com als einen der alternativen Domainnamen

enthalten. Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen (CNAMEs) im Amazon CloudFront Developer Guide.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Datensatztyp und einen mit dem Wert AAAA — IPv6 Adresse. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

App-Runner-Dienst

Führen Sie für den App Runner-Dienst einen der folgenden Schritte aus:

- Wenn Sie dasselbe Konto verwendet haben, um Ihre Route 53-Hosting-Zone und Ihren App Runner-Dienst zu erstellen AWS-Region, wählen Sie den und dann den Domainnamen der Umgebung, in die Sie den Verkehr weiterleiten möchten, aus der Liste aus.
- Wenn Sie verschiedene Konten verwendet haben, um Ihre von Route 53 gehostete Zone und Ihren App Runner zu erstellen, geben Sie den benutzerdefinierten Domainnamen ein. Weitere Informationen finden Sie unter Verwalten benutzerdefinierter Domainnamen für App Runner.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen eines App Runners verwendet haben, wird der App Runner nicht in der Liste der Endpoints angezeigt.

Weitere Informationen finden Sie unter Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen App-Runner-Dienst.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn der Domänenname für Ihre Elastic Beanstalk-Umgebung die Region enthält, in der Sie die Umgebung bereitgestellt haben, können Sie einen Aliasdatensatz erstellen, der Datenverkehr an die Umgebung weiterleitet. Der Domänenname `my-environment.us-west-2.elasticbeanstalk.com` ist beispielsweise ein regionalisierter Domänenname.

> **Important**
>
> Für Umgebungen, die vor Anfang 2016 erstellt wurden, enthält der Domänenname die Region nicht. Um Datenverkehr an diese Umgebungen zu leiten, müssen Sie einen CNAME-Datensatz anstelle eines Alias-Datensatzes erstellen. Beachten Sie, dass es nicht möglich ist, einen CNAME-Datensatz für den Stammdomänennamen zu erstellen. Wenn der Domainname beispielsweise example.com ist, können Sie einen Datensatz erstellen, der den Datenverkehr für acme.example.com an Ihre Elastic Beanstalk-

Umgebung leitet. Sie können jedoch keinen Datensatz erstellen, der den Datenverkehr für example.com an Ihre Elastic Beanstalk-Umgebung leitet.

Im Fall von Elastic-Beanstalk-Umgebungen mit regionalisierten Subdomänen führen Sie einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihrer Elastic-Beanstalk-Umgebung dasselbe Konto verwendet haben – Wählen Sie Endpunkt und anschließend eine Umgebung aus der Liste aus. Bei einer großen Anzahl von Umgebungen können Sie die ersten Zeichen des CNAME-Attributs für die Umgebung eingeben, um die Liste zu filtern.
- Wenn Sie unterschiedliche Konten verwendet haben, um Ihre Route-53-gehostete Zone und Ihre Elastic-Beanstalk-Umgebung zu erstellen – Geben Sie das CNAME-Attribut für die Elastic-Beanstalk-Umgebung ein.

Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an eine AWS Elastic Beanstalk Umgebung.

ELB-Load Balancer

Führen Sie im Fall von ELB-Load Balancern einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung der gehostete Route-53-Zone und Ihres Load Balancer dasselbe Konto verwendet haben – Wählen Sie Endpunkt und anschließend einen Load Balancer aus der Liste aus. Bei einer großen Anzahl von Load Balancern können Sie die ersten Zeichen des DNS-Namens eingeben, um die Liste zu filtern.
- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihres Load Balancer verschiedene Konten verwendet haben – Geben Sie den Wert ein, den Sie im Verfahren Abrufen des DNS-Namens für einen Elastic Load Balancing Load Balancer erhalten haben.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen eines Load Balancers verwendet haben, wird der Load Balancer nicht in der Liste der Endpoints angezeigt.

  Wenn Sie für die Erstellung der aktuellen gehosteten Zone ein Konto und für die Erstellung all Ihrer Load Balancer ein oder mehrere andere Konten verwendet haben, wird in der Liste Endpunkte Keine Ziele verfügbar unter Elastic Load Balancer angezeigt.

Sie müssen dualstack. für Anwendung und Classic Load Balancer aus einem anderen Konto voranstellen. Wenn ein Client, z. B. ein Webbrowser, die IP-Adresse für Ihren Domainnamen

(example.com) oder Ihren Subdomainnamen (www.example.com) anfordert, kann der Client eine IPv4 Adresse (einen A-Datensatz), eine IPv6 Adresse (einen AAAA-Eintrag) oder beides IPv4 und IPv6 Adressen (in separaten Anfragen) anfordern. Die Qualifizierung dualstack. ermöglicht Route 53, mit der jeweiligen IP-Adresse für Ihren Load Balancer zu antworten, abhängig vom IP-Adressenformat, das der Client angefordert hat.

Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr an einen ELB Load Balancer.

AWS Beschleuniger von Global Accelerator

Geben Sie für AWS Global Accelerator-Beschleuniger den DNS-Namen für den Accelerator ein. Sie können den DNS-Namen eines Accelerators eingeben, den Sie mit dem aktuellen AWS Konto oder mit einem anderen AWS Konto erstellt haben.

Amazon-S3-Buckets

Im Fall von Amazon-S3-Buckets, die als Website-Endpunkte konfiguriert sind, führen Sie einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihres Amazon-S3-Buckets dasselbe Konto verwendet haben – Wählen Sie Alias Endpunkt und anschließend einen Bucket aus der Liste aus. Bei einer großen Anzahl von Buckets können Sie die ersten Zeichen des DNS-Namens eingeben, um die Liste zu filtern.

  Der Wert von Endpunkt ändert sich für Ihren Bucket in den Amazon-S3-Website-Endpunkt.
- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihres Amazon-S3-Buckets verschiedene Konten verwendet haben – Geben Sie den Namen der Region ein, in der Sie Ihren S3 Bucket erstellt haben. Verwenden Sie den entsprechenden Wert aus der Spalte Website-Endpunkt in der Tabelle Amazon-S3-Website-Endpunkte im Allgemeine Amazon Web Services-Referenz.

  Wenn Sie für die Erstellung Ihrer Amazon S3 S3-Buckets andere AWS Konten als das aktuelle Konto verwendet haben, wird der Bucket nicht in der Liste der Endpoints angezeigt.

Sie müssen den Bucket für Website-Hosting konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Buckets für Website-Hosting im Benutzerhandbuch für Amazon Simple Storage Service.

Der Name des Datensatzes muss mit dem Namen Ihres Amazon-S3-Buckets übereinstimmen. Wenn der Name des Amazon-S3-Buckets beispielsweise acme.example.com lautet, muss der Name dieses Datensatzes ebenfalls acme.example.com lauten.

In einer Gruppe mit gewichteten Alias-, Latenz-Alias-, Failover-Alias- oder Geolocation-Alias-Datensätzen können Sie nur einen Datensatz erstellen, der Abfragen an einen Amazon-S3-Bucket weiterleitet. Der Grund hierfür ist, dass der Name des Datensatzes mit dem Namen des Buckets übereinstimmen muss und Bucketnamen global eindeutig sein müssen.

OpenSearch Amazon-Dienst

Führen Sie für OpenSearch Service einen der folgenden Schritte aus:

- OpenSearch Benutzerdefinierte Dienstdomäne: Der Name des Eintrags muss mit der benutzerdefinierten Domäne übereinstimmen. Wenn der Name Ihrer benutzerdefinierten Domain beispielsweise test.example.com lautet, muss der Name dieses Datensatzes auch test.example.com lauten.
- Wenn Sie dasselbe Konto verwendet haben, um Ihre Route 53-Hosting-Zone und Ihre OpenSearch Service-Domain zu erstellen AWS-Region, wählen Sie die und dann den Domainnamen aus.
- Wenn Sie unterschiedliche Konten verwendet haben, um Ihre Route 53-Hosting-Zone und Ihre OpenSearch Service-Domain zu erstellen, geben Sie den benutzerdefinierten Domainnamen ein. Weitere Informationen finden Sie unter Benutzerdefinierten Endpunkt erstellen.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen einer OpenSearch Dienstdomäne verwendet haben, wird die Domain nicht in der Liste der Endpoints angezeigt.

  Wenn Sie ein Konto verwendet haben, um die aktuelle Hosting-Zone zu erstellen, und ein oder mehrere verschiedene Konten, um all Ihre OpenSearch Service-Domains zu erstellen, wird in der Liste Endpoints unter OpenSearch Service die Option Keine Ziele verfügbar angezeigt.

Weitere Informationen finden Sie unter Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an einen Amazon OpenSearch Service-Domain-Endpunkt.

Amazon-VPC-Schnittstellenendpunkte

Im Fall von Amazon-VPC-Schnittstellenendpunkten führen Sie einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihres Schnittstellenendpunkts dasselbe Konto verwendet haben – Wählen Sie Endpunkt und anschließend einen Schnittstellenendpunkt aus der Liste aus. Bei einer großen Anzahl von Schnittstellenendpunkten können Sie die ersten Zeichen des DNS-Namens eingeben, um die Liste zu filtern.

- Wenn Sie verschiedene Konten verwendet haben, um Ihre Route 53-Hosting-Zone und Ihren Schnittstellenendpunkt zu erstellen, geben Sie den DNS-Hostnamen für den Schnittstellenendpunkt ein, z. B. vpce-123456789abcdef01- example-us-east -1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com.

  Wenn Sie ein AWS Konto zum Erstellen der aktuellen Hosting-Zone und ein anderes Konto zum Erstellen eines Schnittstellenendpunkts verwendet haben, wird der Schnittstellenendpunkt nicht in der Endpunktliste unter VPC-Endpoints angezeigt.

  Wenn Sie für die Erstellung der aktuellen gehosteten Zone ein Konto und für die Erstellung all Ihrer Schnittstellenendpunkte ein oder mehrere Konten verwendet haben, wird in der Liste Endpunkte Keine Ziele verfügbar unter VPC-Endpunkte angezeigt.

  Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an einen Amazon-Virtual-Private Cloud-Schnittstellenendpunkt unter Verwendung Ihres Domainnamens.

Datensätze in dieser gehosteten Zone

Wählen Sie für Datensätze in dieser gehosteten Zone Endpunkt und anschließend den jeweiligen Datensatz aus. Bei einer großen Anzahl von Datensätzen können Sie die ersten Zeichen des Namens eingeben, um die Liste zu filtern.

Wenn die gehostete Zone nur die NS- und SOA-Standarddatensätze enthält, wird in der Liste Endpunkte Keine Ziele verfügbar angezeigt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz erstellen, der denselben Namen wie die gehostete Zone hat (Zonen-Apex), können Sie keinen Datensatz auswählen, dessen Wert für Datensatztyp CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Spezifische Werte für einfache Datensätze

Beim Erstellen einfacher Datensätze geben Sie die folgenden Werte an.

Themen

Routing-Richtlinie

Klicken Sie auf Einfaches Routing.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6

- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- NS – Namenserver

  Der Domänenname eines Namens-Servers wie ns1.example.com.

  > **Note**
  >
  > Sie können einen NS-Datensatz nur mit einfacher Routing-Richtlinie angeben.

- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den Wert für Datensatztyp danach aus, wie Route 53 auf DNS-Abfragen antworten soll.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven

Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Spezifische Werte für einfache Aliasdatensätze

Beim Erstellen von Aliasdatensätzen geben Sie die folgenden Werte an. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

> **Note**
>
> Wenn Sie Route 53 in der verwenden AWS GovCloud (US) Region, hat diese Funktion einige Einschränkungen. Weitere Informationen finden Sie auf der Amazon-Route-53-Seite im AWS GovCloud (US) -Benutzerhandbuch.

Themen

- Routing-Richtlinie
- Datensatzname
- Bewerten/Weiterleiten des Datenverkehrs an
- Datensatztyp
- Evaluate Target Health

Routing-Richtlinie

Klicken Sie auf Einfaches Routing.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, zu der Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unter Allgemeine Werte für Aliasdatensätze für den value/route Datenverkehr.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr an bestimmte AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, an die Sie den Verkehr weiterleiten:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten, dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Evaluate Target Health

Wenn der Wert der Routing policy (Routing-Richtlinie) Simple (Einfach) ist, können Sie entweder No (Nein) oder den Standardwert Ja auswählen, da Evaluate target health (Zielzustand bewerten) keine Auswirkung auf einfaches Routing hat. Wenn es nur einen Datensatz mit einem bestimmten Namen und Typ gibt, antwortet Route 53 auf DNS-Abfragen mittels der Werte in diesem Datensatz, unabhängig davon, ob die Ressource fehlerfrei ist.

Bei anderen Routing-Richtlinien bestimmt Evaluate target health, ob Route 53 den Zustand der Ressource überprüft, auf die sich der Aliaseintrag bezieht:

- Dienste, bei denen die Bewertung des Zielzustands betriebliche Vorteile bietet: Bei Load Balancers (ELB) und AWS Elastic Beanstalk Umgebungen mit Load Balancers kann Route 53 den Verkehr von fehlerhaften Ressourcen wegleiten, wenn die Option Zielintegrität auswerten auf Ja gesetzt wird.
- Hochverfügbare Services: Für Services wie Amazon S3 S3-Buckets, VPC-Schnittstellenendpunkte, Amazon API Gateway AWS Global Accelerator, Amazon OpenSearch Service und Amazon VPC Lattice bietet Evaluate Target Health keinen betrieblichen Vorteil, da diese Services auf

Hochverfügbarkeit ausgelegt sind. Verwenden Sie für Failover-Szenarien mit diesen Diensten stattdessen Route 53 53-Zustandsprüfungen.

Ausführliche Informationen darüber, wie Evaluate Target Health mit verschiedenen AWS Diensten funktioniert, finden Sie in der EvaluateTargetHealthDokumentation in der API-Referenz.

Spezifische Werte für Failover-Datensätze

Beim Erstellen von Failover-Datensätzen geben Sie die folgenden Werte an.

> **Note**
>
> Weitere Informationen zum Erstellen von Failover-Datensätzen in einer privaten gehosteten Zone finden Sie unter Konfigurieren von Failover in einer privaten gehosteten Zone.

Themen

- Routing-Richtlinie
- Datensatzname
- Datensatztyp
- TTL (Sekunden)
- Bewerten/Weiterleiten des Datenverkehrs an
- Failover-Datensatztyp
- Zustandsprüfung
- Datensatz-ID

Routing-Richtlinie

Klicken Sie auf Failover.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für beide Datensätze in der Gruppe von Failover-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie für die primären und sekundären Failover-Datensätze denselben Wert aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6

- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Failover-Datensatztyp

Wählen Sie den passenden Wert für diesen Datensatz aus. Damit der Failover-Prozess ordnungsgemäß funktionieren kann, müssen Sie einen primären und einen sekundären Failover-Datensatz erstellen.

Sie können keine Nicht-Failover-Datensätze erstellen, die über die gleichen Werte wie Failover-Datensätze für Datensatzname und Datensatztyp verfügen.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain Name (Domänenname) mit dem Namen der Datensätze übereinstimmt, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung nicht planbar.

Datensatz-ID

Geben Sie einen Wert ein, der die primären und sekundären Datensätze eindeutig identifiziert.

Spezifische Werte für Failover-Aliasdatensätze

Beim Erstellen von Failover-Aliasdatensätzen geben Sie die folgenden Werte an.

Weitere Informationen finden Sie unter den folgenden Themen:

- Weitere Informationen zum Erstellen von Failover-Datensätzen in einer privaten gehosteten Zone finden Sie unter Konfigurieren von Failover in einer privaten gehosteten Zone.
- Weitere Informationen über Alias-Datensätze finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

Routing-Richtlinie

Klicken Sie auf Failover.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für beide Datensätze in der Gruppe von Failover-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, zu der Sie den Verkehr weiterleiten. Wählen Sie für die primären und sekundären Failover-Datensätze denselben Wert aus:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten, dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unter Allgemeine Werte für Aliasdatensätze für den value/route Datenverkehr.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr an bestimmte AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

> **Note**
>
> Bei der Erstellung von primären und sekundären Failover-Datensätzen können Sie optional einen Failover- und einen Failover-Alias-Datensatz erstellen, die dieselben Werte für Name und Datensatztyp haben. Wenn Sie Failover- und Failover-Alias-Datensätze mischen, kann jeder davon der primäre Datensatz sein.

Failover-Datensatztyp

Wählen Sie den passenden Wert für diesen Datensatz aus. Damit der Failover-Prozess ordnungsgemäß funktionieren kann, müssen Sie einen primären und einen sekundären Failover-Datensatz erstellen.

Sie können keine Nicht-Failover-Datensätze erstellen, die über die gleichen Werte wie Failover-Datensätze für Datensatzname und Datensatztyp verfügen.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain Name (Domänenname) mit dem Namen der Datensätze übereinstimmt, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung nicht planbar.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Zielzustand bewerten auf Ja, wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können die Option Zielintegrität bewerten nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancer — Wenn Sie in Endpoint einen ELB Classic Load Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendung und Network Load Balancer – Wenn Sie eine ELB-Anwendung oder einen Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss eine Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.
  - Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen

im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der die primären und sekundären Datensätze eindeutig identifiziert.

Spezifische Werte für Geolocation-Datensätze

Beim Erstellen von Geolocation-Datensätzen geben Sie die folgenden Werte an.

Themen

Routing-Richtlinie

Wählen Sie Geolocation aus.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von Geolocation-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie für alle Datensätze in der Gruppe von Geolocation-Datensätzen denselben Namen aus:

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)

- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Ort

Bei der Konfiguration von Route 53 für Antworten auf DNS-Abfragen auf Basis des Standorts, von dem die Abfragen stammen, wählen Sie den Kontinent oder das Land aus, für den bzw. das Route 53 mit den Einstellungen in diesem Datensatz antworten soll. Wenn Route 53 auf DNS-Abfragen für einzelne Bundesstaaten in den Vereinigten Staaten antworten soll, wählen Sie United States (USA) in der Liste Location (Ort) und den Bundesstaat in der Liste Sublocation (Standort) aus.

Wählen Sie für eine private gehostete Zone den Kontinent, das Land oder die Unterabteilung aus, die dem, in dem sich Ihre Ressource befindet AWS-Region , am nächsten liegt. Wenn sich Ihre Ressource beispielsweise in us-east-1 befindet, können Sie Nordamerika, USA oder Virginia angeben.

> **Important**
>
> Es wird empfohlen, einen Geolocation-Datensatz mit dem Wert Standard für Standort zu erstellen. Dies deckt geographische Standorte ab, für die Sie keine Datensätze erstellt haben, sowie IP-Adressen, für die Route 53 keinen Standort identifizieren kann.

Sie können keine Nicht-Geolocation-Datensätze erstellen, die für Datensatzname und Datensatztyp die gleichen Werte wie Geolocation-Datensätze aufweisen.

Weitere Informationen finden Sie unter Geolocation-Routing.

Dies sind die Länder, die Amazon Route 53 dem jeweiligen Kontinent zuordnet. Die Ländercodes entsprechen ISO 3166. Weitere Informationen finden Sie im Wikipedia-Artikel zu ISO 3166-1 Alpha-2:

Afrika (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antarktika (AN)

AQ, GS, TF

Asien (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

Europa (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

> **Note**
>
> Einige Anbieter gehen davon aus, dass TR in Asien angesiedelt ist, und die IP-Adressen werden dies widerspiegeln.

Nordamerika (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

Ozeanien (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

Südamerika (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53 unterstützt nicht die Erstellung von Geolokalisierungsdatensätzen für die folgenden Länder: Bouvetinsel (BV), Weihnachtsinsel (CX), Westsahara (EH) und Heard Island and McDonald Islands (HM). Für diese Länder stehen keine Daten zu IP-Adressen zur Verfügung.

US-Staaten

Wenn Route 53 auf DNS-Abfragen auf Basis des Bundesstaats in den Vereinigten Staaten, aus dem die Abfragen stammen, antworten soll, wählen Sie den Bundesstaat in der Liste USA-Staaten aus. US-Territorien (zum Beispiel Puerto Rico) werden in der Liste Location (Ort) als Länder aufgeführt.

> **Important**
>
> Einige IP-Adressen sind mit den Vereinigten Staaten verknüpft, aber nicht mit einem einzelnen Bundesstaat. Wenn Sie Datensätze für sämtliche Bundesstaaten der Vereinigten Staaten erstellen, empfehlen wir, auch einen Datensatz für die Vereinigten Staaten zu erstellen, um diese nicht verknüpften IP-Adressen weiterzuleiten. Wenn Sie keinen Datensatz für die Vereinigten Staaten erstellen, antwortet Route 53 auf DNS-Abfragen von nicht verknüpften IP-Adressen der Vereinigten Staaten mit den Einstellungen aus dem standardmäßigen Geolocation-Datensatz (sofern von Ihnen erstellt) oder mit der Information, dass keine Antwort erfolgt.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover- oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die

Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.

- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain Name (Domänenname) mit dem Namen der Datensätze übereinstimmt, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung nicht planbar.

Wenn es einen fehlerhaften Endpunkt in Geolocation-Datensätzen gibt, sucht Route 53 nach einem Datensatz für die größere verknüpfte geografische Region. Angenommen, Sie besitzen Datensätze für einen Bundesstaat der Vereinigten Staaten, für die Vereinigten Staaten, für Nordamerika und für alle Standorte (Location (Standort) ist Default (Standard)). Wenn der Endpunkt für den Bundesstaatdatensatz fehlerhaft ist, prüft Route 53 der Reihe nach die Datensätze für die Vereinigten Staaten, für Nordamerika und für alle Standorte, bis ein Datensatz mit einem fehlerfreien Endpunkt gefunden wird. Wenn alle Datensätze einschließlich des Datensatzes für alle Standorte fehlerhaft sind, antwortet Route 53 auf die DNS-Abfrage mittels des Werts für den Datensatz für die kleinste geografische Region.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von Geolocation-Datensätzen eindeutig identifiziert.

Spezifische Werte für Geolocation-Aliasdatensätze

Beim Erstellen von Geolocation-Aliasdatensätzen geben Sie die folgenden Werte an.

Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

Routing-Richtlinie

Wählen Sie Geolocation aus.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von Geolocation-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, zu der Sie den Verkehr weiterleiten. Wählen Sie für alle Datensätze in der Gruppe von Geolocation-Datensätzen denselben Namen aus:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie A — IPv4 Adresse oder AAAA — IPv6 Adresse

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten,

dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unterBewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr zu bestimmten AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Speicherort

Bei der Konfiguration von Route 53 für Antworten auf DNS-Abfragen auf Basis des Standorts, von dem die Abfragen stammen, wählen Sie den Kontinent oder das Land aus, für den bzw. das Route 53 mit den Einstellungen in diesem Datensatz antworten soll. Wenn Route 53 auf DNS-Abfragen für einzelne Bundesstaaten in den Vereinigten Staaten antworten soll, wählen Sie United States (USA) in der Liste Location (Ort) und den Bundesstaat in der Liste U.S. States (USA) aus.

Wählen Sie für eine private gehostete Zone den Kontinent, das Land oder die Unterteilung aus, die dem, in dem sich Ihre Ressource befindet AWS-Region , am nächsten liegt. Wenn sich Ihre Ressource beispielsweise in us-east-1 befindet, können Sie Nordamerika, USA oder Virginia angeben.

Important

Es wird empfohlen, einen Geolocation-Datensatz mit dem Wert Standard für Standort zu erstellen. Dies deckt geographische Standorte ab, für die Sie keine Datensätze erstellt haben, sowie IP-Adressen, für die Route 53 keinen Standort identifizieren kann.

Sie können keine Nicht-Geolocation-Datensätze erstellen, die für Datensatzname und Datensatztyp die gleichen Werte wie Geolocation-Datensätze aufweisen.

Weitere Informationen finden Sie unter Geolocation-Routing.

Dies sind die Länder, die Amazon Route 53 dem jeweiligen Kontinent zuordnet. Die Ländercodes entsprechen ISO 3166. Weitere Informationen finden Sie im Wikipedia-Artikel zu ISO 3166-1 Alpha-2:

Afrika (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antarktika (AN)

AQ, GS, TF

Asien (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

Europa (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

> **Note**
>
> Einige Anbieter gehen davon aus, dass TR in Asien angesiedelt ist, und die IP-Adressen werden dies widerspiegeln.

Nordamerika (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

Ozeanien (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

Südamerika (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53 unterstützt nicht die Erstellung von Geolokalisierungsdatensätzen für die folgenden Länder: Bouvetinsel (BV), Weihnachtsinsel (CX), Westsahara (EH) und Heard Island and McDonald Islands (HM). Für diese Länder stehen keine Daten zu IP-Adressen zur Verfügung.

US-Staaten

Wenn Route 53 auf DNS-Abfragen auf Basis des Bundesstaats in den Vereinigten Staaten, aus dem die Abfragen stammen, antworten soll, wählen Sie den Bundesstaat in der Liste USA-Staaten aus. US-Territorien (zum Beispiel Puerto Rico) werden in der Liste Location (Ort) als Länder aufgeführt.

> **Important**
>
> Einige IP-Adressen sind mit den Vereinigten Staaten verknüpft, aber nicht mit einem einzelnen Bundesstaat. Wenn Sie Datensätze für sämtliche Bundesstaaten der Vereinigten Staaten erstellen, empfehlen wir, auch einen Datensatz für die Vereinigten Staaten zu erstellen, um diese nicht verknüpften IP-Adressen weiterzuleiten. Wenn Sie keinen Datensatz für die Vereinigten Staaten erstellen, antwortet Route 53 auf DNS-Abfragen von nicht verknüpften IP-Adressen der Vereinigten Staaten mit den Einstellungen aus dem standardmäßigen Geolocation-Datensatz (sofern von Ihnen erstellt) oder mit der Information, dass keine Antwort erfolgt.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung

angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Wenn es einen fehlerhaften Endpunkt in Geolocation-Datensätzen gibt, sucht Route 53 nach einem Datensatz für die größere verknüpfte geografische Region. Angenommen, Sie besitzen Datensätze für einen Bundesstaat der Vereinigten Staaten, für die Vereinigten Staaten, für Nordamerika und für alle Standorte (Location (Standort) ist Default (Standard)). Wenn der Endpunkt für den Bundesstaatdatensatz fehlerhaft ist, prüft Route 53 der Reihe nach die Datensätze für die Vereinigten Staaten, für Nordamerika und für alle Standorte, bis ein Datensatz mit einem fehlerfreien Endpunkt gefunden wird. Wenn alle Datensätze einschließlich des Datensatzes für alle Standorte fehlerhaft sind, antwortet Route 53 auf die DNS-Abfrage mittels des Werts für den Datensatz für die kleinste geografische Region.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Evaluate target health (Zielzustand bewerten) auf Yes (Ja), wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können die Option Zielintegrität bewerten nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancers — Wenn Sie einen ELB Classic Load Balancer in Endpoint angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie „Zielstatus bewerten“ auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendungs- und Network Load Balancer – Wenn Sie einen ELB-Anwendungs- oder -Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss jede Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.
  - Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von Geolocation-Datensätzen eindeutig identifiziert.

Spezifische Werte für Geoproximitätsdatensätze

Wenn Sie Geoproximitätsdatensätze erstellen, geben Sie die folgenden Werte an.

Themen

Routing-Richtlinie

Wählen Sie Geoproximity aus.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie denselben Namen für alle Datensätze in der Gruppe der Geoproximitätsdatensätze ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie denselben Wert für alle Datensätze in der Gruppe der Geoproximitätsdatensätze aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — Adresse IPv4
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)

- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Endpunktstandort

Sie können den Speicherort des Ressourcenendpunkts mit einer der folgenden Methoden angeben:

Benutzerdefinierte Koordinaten

Geben Sie den Längen- und Breitengrad für ein geografisches Gebiet an.

AWS-Region

Wählen Sie eine verfügbare Region aus der Standortliste aus.

Weitere Informationen zu den Regionen finden Sie unter AWS Globale Infrastruktur.

AWS Lokale Zonengruppe

Wählen Sie eine verfügbare lokale Zonengruppe aus der Standortliste aus.

Weitere Informationen zu Local Zones finden Sie unter Available Local Zones im AWS Local Zones User Guide. Eine lokale Zonengruppe ist normalerweise die lokale Zone ohne das Endzeichen. Wenn die lokale Zone beispielsweise die lokale Zone ist, ist es `us-east-1-bue-1a` die lokale Zonengruppe`us-east-1-bue-1`.

Sie können die Local Zones Group auch für eine bestimmte Local Zone identifizieren, indem Sie den describe-availability-zonesCLI-Befehl verwenden:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Dieser Befehl gibt: zurück und gibt an`"GroupName": "us-west-2-den-1"`, dass die Local Zone `us-west-2-den-1a` zur Local Zone Group gehört`us-west-2-den-1`.

Sie können keine Geoproximitätsdatensätze erstellen, die dieselben Werte für Datensatzname und Datensatztyp wie Geoproximitätsdatensätze haben.

Sie können auch nicht zwei Geoproximity-Ressourcendatensätze erstellen, die denselben Standort für denselben Datensatznamen und Datensatztyp angeben.

Bias

Durch eine Abweichung wird ein geografisches Gebiet, von dem aus die Route 53 den Verkehr zu einer Ressource weiterleitet, entweder vergrößert oder verkleinert. Eine positive Tendenz erweitert den Bereich, und eine negative Tendenz verkleinert ihn. Weitere Informationen finden Sie unter So verwendet Amazon Route 53 Bias-Werte.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Ja für Evaluate Target Health für einen Aliasdatensatz oder die Datensätze in einer Gruppe von Failover-Alias, Geolocation-Alias, Geoproximity-Alias, Latenzalias, IP-basiertem Alias oder gewichtetem Aliasdatensatz. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die

referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain Name (Domänenname) mit dem Namen der Datensätze übereinstimmt, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung nicht planbar.

Wenn ein Endpunkt fehlerhaft ist, sucht Route 53 bei Geoproximitätsdatensätzen nach einem Endpunkt, der sich am nächsten befindet und noch fehlerfrei ist.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe der Geoproximitätsdatensätze eindeutig identifiziert.

Spezifische Werte für Geoproximitäts-Aliasdatensätze

Wenn Sie Geoproximity-Aliasdatensätze erstellen, geben Sie die folgenden Werte an.

Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

Routing-Richtlinie

Wählen Sie Geoproximity.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie denselben Namen für alle Datensätze in der Gruppe der Geoproximitätsdatensätze ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, zu der Sie den Verkehr weiterleiten. Wählen Sie denselben Wert für alle Datensätze in der Gruppe der Geoproximitätsdatensätze aus:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie A — IPv4 Adresse oder AAAA — IPv6 Adresse

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten,

dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unterBewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr zu bestimmten AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Endpunktstandort

Sie können den Standort des Ressourcenendpunkts mit einer der folgenden Methoden angeben:

Benutzerdefinierte Koordinaten

Geben Sie den Längen- und Breitengrad für ein geografisches Gebiet an.

AWS-Region

Wählen Sie eine verfügbare Region aus der Standortliste aus.

Weitere Informationen zu den Regionen finden Sie unter AWS Globale Infrastruktur.

AWS Lokale Zonengruppe

Wählen Sie eine verfügbare lokale Zonenregion aus der Standortliste aus.

Weitere Informationen zu Local Zones finden Sie unter Available Local Zones im AWS Local Zones User Guide. Eine lokale Zonengruppe ist normalerweise die lokale Zone ohne das Endzeichen. Wenn die lokale Zone beispielsweise die lokale Zone ist, ist es `us-east-1-bue-1a` die lokale Zonengruppe`us-east-1-bue-1`.

Sie können die Local Zones Group auch für eine bestimmte Local Zone identifizieren, indem Sie den describe-availability-zonesCLI-Befehl verwenden:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Dieser Befehl gibt: zurück und gibt an`"GroupName": "us-west-2-den-1"`, dass die Local Zone `us-west-2-den-1a` zur Local Zone Group gehört`us-west-2-den-1`.

Sie können keine Geoproximitätsdatensätze erstellen, die dieselben Werte für Datensatzname und Datensatztyp wie Geoproximitätsdatensätze haben.

Sie können auch nicht zwei Geoproximity-Ressourcendatensätze erstellen, die denselben Standort für denselben Datensatznamen und Datensatztyp angeben.

Weitere Informationen finden Sie unter .html available-local-zones

Bias

Durch eine Verzerrung wird ein geografisches Gebiet, von dem aus die Route 53 den Verkehr zu einer Ressource weiterleitet, entweder vergrößert oder verkleinert. Eine positive Tendenz erweitert den Bereich, und eine negative Tendenz verkleinert ihn. Weitere Informationen finden Sie unter So verwendet Amazon Route 53 Bias-Werte.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete

Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.

- Sie wählen Ja für Zielintegrität für einen Aliasdatensatz oder die Datensätze in einer Gruppe von Failover-Alias, Geolocation-Alias, Geoproximity-Alias, Latenz-Alias, IP-basiertem Alias oder gewichtetem Aliasdatensatz auswerten. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Wenn ein Endpunkt fehlerhaft ist, sucht Route 53 bei Geoproximitätsdatensätzen nach einem Endpunkt, der sich am nächsten befindet und noch fehlerfrei ist.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Evaluate target health (Zielzustand bewerten) auf Yes (Ja), wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können die Option Zielintegrität bewerten nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancers — Wenn Sie einen ELB Classic Load Balancer in Endpoint angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie „Zielstatus bewerten“ auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendungs- und Network Load Balancer – Wenn Sie einen ELB-Anwendungs- oder -Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss jede Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.

- Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe der Geoproximitätsdatensätze eindeutig identifiziert.

Spezifische Werte für Latenz-Datensätze

Beim Erstellen von Latenz-Datensätzen geben Sie die folgenden Werte an.

Themen

Routing-Richtlinie

Klicken Sie auf Latenz.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von Latenz-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den Wert für Typ danach aus, wie Route 53 auf DNS-Abfragen antworten soll.

Wählen Sie für alle Datensätze in der Gruppe von Latenz-Datensätzen denselben Namen aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)

- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Region

Die EC2 Amazon-Region, in der sich die Ressource befindet, die Sie in diesem Datensatz angegeben haben. Route 53 empfiehlt eine EC2 Amazon-Region auf der Grundlage anderer Werte, die Sie angegeben haben. Dies gilt auch für privat gehostete Zonen. Wir empfehlen, diesen Wert nicht zu ändern.

Beachten Sie Folgendes:

- Sie können nur einen Latenzdatensatz für jede EC2 Amazon-Region erstellen.
- Sie müssen keine Latenzdatensätze für alle EC2 Amazon-Regionen erstellen. Route 53 wählt aus den Regionen, für die Sie Latenzdatensätze erstellen, die Region mit der besten Latenz aus.
- Sie können keine Datensätze ohne Latenz erstellen, die über dieselben Werte wie Latenzdatensätze für Datensatzname und Datensatztyp verfügen.
- Wenn Sie einen Datensatz erstellen, der mit der Region cn-north-1 markiert ist, antwortet Route 53 unabhängig von der Latenz immer auf Abfragen aus China mit diesem Datensatz.

Weitere Informationen zum Verwenden von Latenz-Datensätzen finden Sie unter Latenzbasiertes Routing.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover- oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von Latenz-Datensätzen eindeutig identifiziert.

Spezifische Werte für Latenz-Aliasdatensätze

Beim Erstellen von Latenz-Aliasdatensätzen geben Sie die folgenden Werte an.

Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

Routing-Richtlinie

Klicken Sie auf Latenz.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von Latenz-Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, an die Sie den Verkehr weiterleiten:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie A — IPv4 Adresse oder AAAA — IPv6 Adresse

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten,

dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Wählen Sie für alle Datensätze in der Gruppe von Latenz-Datensätzen denselben Namen aus.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unter Allgemeine Werte für Aliasdatensätze für den value/route Datenverkehr.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr an bestimmte AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Region

Die EC2 Amazon-Region, in der sich die Ressource befindet, die Sie in diesem Datensatz angegeben haben. Route 53 empfiehlt eine EC2 Amazon-Region auf der Grundlage anderer Werte, die Sie angegeben haben. Dies gilt auch für privat gehostete Zonen. Wir empfehlen, diesen Wert nicht zu ändern.

Beachten Sie Folgendes:

- Sie können nur einen Latenzdatensatz für jede EC2 Amazon-Region erstellen.
- Sie müssen keine Latenzdatensätze für alle EC2 Amazon-Regionen erstellen. Route 53 wählt aus den Regionen, für die Sie Latenzdatensätze erstellen, die Region mit der besten Latenz aus.
- Sie können keine Datensätze ohne Latenz erstellen, die über dieselben Werte wie Latenzdatensätze für Datensatzname und Datensatztyp verfügen.
- Wenn Sie einen Datensatz erstellen, der mit der Region cn-north-1 markiert ist, antwortet Route 53 unabhängig von der Latenz immer auf Abfragen aus China mit diesem Datensatz.

Weitere Informationen zum Verwenden von Latenz-Datensätzen finden Sie unter Latenzbasiertes Routing.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain Name (Domänenname) mit dem Namen der Datensätze übereinstimmt, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung nicht planbar.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Zielzustand bewerten auf Ja, wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können Evaluate Target Health nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancers — Wenn Sie einen ELB Classic Load Balancer in Endpoint angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie „Zielstatus bewerten“ auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendungs- und Network Load Balancer – Wenn Sie einen ELB-Anwendungs- oder -Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss jede Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.
  - Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen

im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von Latenz-Datensätzen eindeutig identifiziert.

Spezifische Werte für IP-basierte Datensätze

Beim Erstellen IP-basierter Datensätze geben Sie die folgenden Werte an.

> **Note**
>
> Das Erstellen von IP-basierten Datensätzen in einer privat gehosteten Zone ist zwar erlaubt, wird aber nicht unterstützt.

Themen

Routing-Richtlinie

Wählen Sie IP-based (IP-basiert) aus.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie den gleichen Namen für alle Datensätze in der Gruppe von IP-basierten Datensätzen ein.

CNAME-Datensätze

Wenn Sie einen Datensatz erstellen, der den Wert CNAME für Datensatztyp hat, darf der Name für den Datensatz nicht gleich dem Namen der gehosteten Zone sein.

Sonderzeichen

Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

Platzhalterzeichen

Sie können im Namen ein Sternchenzeichen (*) verwenden. Abhängig von seiner Position im Namen wird das *-Zeichen vom DNS entweder als Platzhalter oder als das *-Zeichen (ASCII 42) behandelt. Weitere Informationen finden Sie unter Verwendung eines Sternchens (*) im Namen von gehosteten Zonen und Datensätzen.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den Wert für Typ danach aus, wie Route 53 auf DNS-Abfragen antworten soll.

Wählen Sie denselben Wert für alle Datensätze in der Gruppe der IP-basierten Datensätze aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie

z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — Adresse IPv4
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Bewerten/Weiterleiten des Datenverkehrs an Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Ort

Der Name des CIDR-Standorts, an dem die Ressource, die Sie in diesem Datensatz angegeben haben, durch die CIDR-Blockwerte innerhalb des CIDR-Standorts angegeben wird.

Weitere Informationen zum Verwenden von IP-basierten Datensätzen finden Sie unter IP-basiertes Routing.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basiertem Alias oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von IP-basierten Datensätzen eindeutig identifiziert.

Spezifische Werte für IP-basierte Aliasdatensätze

Beim Erstellen von IP-basierten Aliasdatensätzen geben Sie die folgenden Werte an.

> **Note**
>
> Das Erstellen von IP-basierten Aliasdatensätzen in einer privat gehosteten Zone ist zwar erlaubt, wird aber nicht unterstützt.

Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

- Routing-Richtlinie
- Datensatzname
- Datensatztyp
- Bewerten/Weiterleiten des Datenverkehrs an
- Speicherort
- Gesundheitscheck
- Evaluate Target Health
- Datensatz-ID

Routing-Richtlinie

Wählen Sie IP-based (IP-basiert) aus.

> **Note**
>
> Das Erstellen von IP-basierten Aliasdatensätzen in einer privat gehosteten Zone ist zwar erlaubt, wird aber nicht unterstützt.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie den gleichen Namen für alle Datensätze in der Gruppe von IP-basierten Datensätzen ein.

CNAME-Datensätze

Wenn Sie einen Datensatz erstellen, der den Wert CNAME für Datensatztyp hat, darf der Name für den Datensatz nicht gleich dem Namen der gehosteten Zone sein.

Aliase für CloudFront Distributionen und Amazon S3 S3-Buckets

Der Wert, den Sie angeben, hängt zum Teil von der AWS Ressource ab, an die Sie den Datenverkehr weiterleiten:

- CloudFront Verteilung — Ihre Distribution muss einen alternativen Domainnamen enthalten, der dem Namen des Eintrags entspricht. Wenn der Name des Datensatzes beispielsweise acme.example.com ist, muss Ihre CloudFront-Verteilung acme.example.com als einen alternativen Domänennamen enthalten. Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen (CNAMEs) im Amazon CloudFront Developer Guide.
- Amazon-S3-Bucket – Der Name des Datensatzes muss mit dem Namen Ihres Amazon-S3-Buckets übereinstimmen. Wenn der Name des Buckets beispielsweise acme.example.com lautet, muss der Name dieses Datensatzes ebenfalls acme.example.com lauten.

  Außerdem müssen Sie den Bucket für das Website-Hosting konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Buckets für Website-Hosting im Benutzerhandbuch für Amazon Simple Storage Service.

Sonderzeichen

Erläuterungen dazu, wie Sie andere Zeichen als a-z, 0-9 und - (Bindestrich) eingeben und wie internationale Domainnamen angegeben werden, erhalten Sie unter Format für DNS-Domänennamen.

Platzhalterzeichen

Sie können im Namen ein Sternchenzeichen (*) verwenden. Abhängig von seiner Position im Namen wird das *-Zeichen vom DNS entweder als Platzhalter oder als das *-Zeichen (ASCII 42)

behandelt. Weitere Informationen finden Sie unter Verwendung eines Sternchens (*) im Namen von gehosteten Zonen und Datensätzen.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, an die Sie den Datenverkehr weiterleiten. Wählen Sie für alle Datensätze in der Gruppe IP-basierter Datensätzen denselben Wert aus.

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie A — IPv4 Adresse oder AAAA — IPv6 Adresse

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten, dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unter Allgemeine Werte für Aliasdatensätze für den value/route Datenverkehr.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr an bestimmte AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Speicherort

Bei der Konfiguration von Route 53 für Antworten auf DNS-Abfragen auf Basis des Standorts, von dem die Abfragen stammen, wählen Sie den CIDR-Standort aus, für den bzw. das Route 53 mit den Einstellungen in diesem Datensatz antworten soll.

> **Important**
>
> Es wird empfohlen, einen IP-basierten Datensatz mit dem Wert Standard für Standort zu erstellen. Dies deckt Standorte ab, für die Sie keine Datensätze erstellt haben, sowie IP-Adressen, für die Route 53 keinen Standort identifizieren kann.

Sie können keine non-IP-based Datensätze erstellen, die dieselben Werte für Datensatzname und Datensatztyp haben wie IP-basierte Datensätze.

Weitere Informationen finden Sie unter IP-basiertes Routing.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, IP-basiertem Alias-, Latenz-Alias oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für

jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Wenn es einen ungesunden Endpunkt in IP-basierten Aliasdatensätzen gibt, sucht Route 53 nach einem Datensatz im größeren verbundenen Standort. Angenommen, Sie besitzen Datensätze für einen Bundesstaat der Vereinigten Staaten, für die Vereinigten Staaten, für Nordamerika und für alle Standorte (Location (Standort) ist Default (Standard)). Wenn der Endpunkt für den Bundesstaatdatensatz fehlerhaft ist, prüft Route 53 der Reihe nach die Datensätze für die Vereinigten Staaten, für Nordamerika und für alle Standorte, bis ein Datensatz mit einem fehlerfreien Endpunkt gefunden wird. Wenn alle Datensätze einschließlich des Datensatzes für alle Standorte fehlerhaft sind, antwortet Route 53 auf die DNS-Abfrage mittels des Werts für den Datensatz für die kleinste geografische Region.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Zielzustand bewerten auf Ja, wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können die Option Zielintegrität bewerten nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancers — Wenn Sie einen ELB Classic Load Balancer in Endpoint angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie „Zielstatus bewerten“ auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendungs- und Network Load Balancer – Wenn Sie einen ELB-Anwendungs- oder -Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss jede Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.
  - Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von IP-basierten Datensätzen eindeutig identifiziert.

Werte für spezifische mehrwertige Antwort-Datensätze

Beim Erstellen mehrwertiger Antwort-Datensätze geben Sie folgende Werte an.

> **Note**
>
> Das Erstellen von mehrwertigen Antwort-Aliasdatensätzen wird nicht unterstützt.

Themen

- Routing-Richtlinie
- Datensatzname
- Datensatztyp
- TTL (Sekunden)
- Bewerten/Weiterleiten des Datenverkehrs an
- Zustandsprüfung
- Datensatz-ID

Routing-Richtlinie

Klicken Sie auf Mehrwertige Antwort.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von mehrwertigen Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie einen beliebigen Wert außer NS und CNAME aus.

Wählen Sie für alle Datensätze in der Gruppe von mehrwertigen Antwort-Datensätzen denselben Namen aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

> **Note**
>
> Wenn Sie zwei oder mehr mehrwertige Antwortdatensätze mit demselben Namen und Typ erstellen, verwenden Sie die Konsole und legen unterschiedliche Werte für TTL fest. Route 53 ändert den Wert von TTL für alle Datensätze auf den letzten angegebenen Wert.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Wenn Sie mehr als einen Wert eingeben, geben Sie jeden Wert in einer separaten Zeile ein.

Sie können den Datenverkehr weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von mehrwertigen Antwort-Datensätzen eindeutig identifiziert.

Spezifische Werte für gewichtete Datensätze

Beim Erstellen von gewichteten Datensätzen geben Sie die folgenden Werte an.

Themen

Routing-Richtlinie

Wählen Sie Weighted (Gewichtet) aus.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von gewichteten Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie für alle Datensätze in der Gruppe von gewichteten Datensätzen denselben Namen aus.

TTL (Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Durch Angabe eines längeren Wertes (z. B. 172800 Sekunden, oder zwei Tage) verringern Sie die Anzahl der Aufrufe, die rekursive DNS-Resolver an Route 53 senden müssen, um die neuesten Informationen in diesem Datensatz zu erhalten. Dies führt zu einer Verringerung der Latenz und Ihrer Rechnung für den Route 53-Service. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Wenn Sie einen längeren Wert als TTL angeben, dauert es allerdings länger, bis Änderungen an dem Datensatz (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern. Wenn Sie Einstellungen für eine Domäne oder Subdomäne ändern, die bereits verwendet wird, wird empfohlen, anfänglich einen kürzeren Wert, wie z. B. 300 Sekunden anzugeben und den Wert zu erhöhen, nachdem Sie bestätigt haben, dass die neuen Einstellungen korrekt sind.

Wenn Sie diesen Datensatz mit einer Zustandsprüfung verknüpfen, empfehlen wir Ihnen eine Time to Live (TTL, Gültigkeitsdauer) von 60 Sekunden oder weniger einzugeben, damit Clients schnell auf Änderungen im Zustandsstatus reagieren.

Sie müssen für alle Datensätze in dieser Gruppe von gewichteten Datensätzen denselben Wert für TTL angeben.

> **Note**
>
> Wenn Sie zwei oder mehr gewichtete Datensätze mit demselben Namen und Typ erstellen und unterschiedliche Werte für TTL festlegen, ändert Route 53 den Wert von TTL für alle Datensätze auf den letzten angegebenen Wert.

Wenn eine Gruppe von gewichteten Datensätzen einen oder mehrere gewichtete Alias-Datensätze enthält, die Datenverkehr an einen ELB-Load Balancer weiterleiten, wird empfohlen, eine TTL von 60 Sekunden für sämtliche gewichteten Nicht-Alias-Datensätze anzugeben, die denselben Namen und Typ haben. Andere Werte als 60 Sekunden (die TTL für Load Balancer) ändern die Auswirkungen der Werte, die Sie für Weight (Gewichtung) angeben.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie einen gültigen Wert für Datensatztyp ein. Sie können für alle Typen außer CNAME mehr als einen Wert eingeben. Fügen Sie jeden Wert in einer separaten Zeile hinzu.

Sie können weiterleiten oder die folgenden Werte angeben:

- A — IPv4 Adresse
- AAAA — Adresse IPv6
- CAA – Certificate Authority Authorization (Autorisierung der Zertifizierungsstelle)
- CNAME – kanonischer Name
- MX – Mail-Austausch
- NAPTR – Name Authority Pointer (Namensautorisierungszeiger)
- PTR – Pointer (Zeiger)
- SPF – Sender Policy Framework (Richtlinien-Framework des Senders)
- SRV – Service-Locator
- TXT – Text

Weitere Informationen zu diesen Werten finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Gewicht

Ein Wert, der das Verhältnis von DNS-Abfragen, auf die Route 53 antwortet, anhand des aktuellen Datensatzes bestimmt. Route 53 berechnet die Summe der Gewichtungen für die Datensätze, die dieselbe Kombination von DNS-Namen und -Typ aufweisen. Route 53 beantwortet dann Abfragen, die auf dem Verhältnis der Gewichtung einer Ressource zur Gesamtsumme basieren.

Sie können keine nicht gewichteten Datensätze erstellen, die über dieselben Werte wie gewichtete Datensätze für Datensatzname und Datensatztyp verfügen.

Geben Sie eine Ganzzahl zwischen 0 und 255 ein. Zum Deaktivieren der Weiterleitung an eine Ressource setzen Sie für Weight (Gewichtung) den Wert 0 fest. Wenn Sie Weight (Gewichtung) für alle Datensätze in der Gruppe auf 0 setzen, wird der Datenverkehr mit gleicher Wahrscheinlichkeit zu allen Ressourcen weitergeleitet. Auf diese Weise wird verhindert, dass Sie die Weiterleitung für eine Gruppe von gewichteten Datensätzen versehentlich deaktivieren.

Wenn Sie Zustandsprüfungen mit gewichteten Datensätzen verknüpfen und Weight (Gewichtung) auf 0 setzen, unterscheidet sich das Resultat. Weitere Informationen finden Sie unter So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind.

Zustandsprüfung

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben die Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain

Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von gewichteten Datensätzen eindeutig identifiziert.

Spezifische Werte für gewichtete Aliasdatensätze

Beim Erstellen von gewichteten Aliasdatensätzen geben Sie die folgenden Werte an. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

Routing-Richtlinie

Klicken Sie auf Gewichtet.

Datensatzname

Geben Sie den Namen der Domäne oder Subdomäne ein, für die Sie Verkehr weiterleiten wollen. Der Standardwert ist der Name der gehosteten Zone.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie für alle Datensätze in der Gruppe von gewichteten Datensätzen denselben Namen ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den entsprechenden Wert basierend auf der AWS Ressource aus, an die Sie den Verkehr weiterleiten:

Benutzerdefinierte regionale API-Gateway-API oder Edge-optimierte API

Wählen Sie A — IPv4 Adresse aus.

Amazon-VPC-Schnittstellenendpunkte

Wählen Sie A — IPv4 Adresse aus.

CloudFront Vertrieb

Wählen Sie A — IPv4 Adresse aus.

Wenn für die Verteilung aktiviert IPv6 ist, erstellen Sie zwei Datensätze, einen mit dem Wert A — IPv4 Adresse für Typ und einen mit dem Wert AAAA — IPv6 Adresse.

App-Runner-Dienst

Wählen Sie A — Adresse IPv4

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A — IPv4 Adresse

ELB-Load Balancer

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Amazon-S3-Bucket

Wählen Sie A — Adresse IPv4

OpenSearch Dienst

Wählen Sie IPv4 A-Adresse oder AAAA-Adresse IPv6

Weiterer Datensatz in dieser gehosteten Zone

Wählen Sie den Typ des Datensatzes aus, für den Sie den Alias erstellen. Es werden alle Typen außer NS und SOA unterstützt.

> **Note**
>
> Wenn Sie einen Aliasdatensatz mit demselben Namen wie die gehostete Zone (Zonen-Apex) erstellen, können Sie den Datenverkehr nicht zu einem Datensatz weiterleiten,

dessen Wert in Type (Typ) CNAME ist. Der Grund hierfür ist, dass der Aliasdatensatz denselben Typ wie der Datensatz haben muss, zu dem Sie den Datenverkehr weiterleiten, und die Erstellung eines CNAME-Datensatzes für den Zonen-Apex wird für einen Aliasdatensatz nicht unterstützt.

Wählen Sie für alle Datensätze in der Gruppe von gewichteten Datensätzen denselben Namen aus.

Bewerten/Weiterleiten des Datenverkehrs an

Der Wert, den Sie aus der Liste auswählen oder den Sie in das Feld eingeben, hängt von der AWS Ressource ab, an die Sie den Verkehr weiterleiten.

Informationen darüber, auf welche AWS Ressourcen Sie abzielen können, finden Sie unter Allgemeine Werte für Aliasdatensätze für den value/route Datenverkehr.

Weitere Informationen zur Konfiguration von Route 53 zur Weiterleitung von Datenverkehr an bestimmte AWS Ressourcen finden Sie unterWeiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Gewicht

Ein Wert, der das Verhältnis von DNS-Abfragen, auf die Route 53 antwortet, anhand des aktuellen Datensatzes bestimmt. Route 53 berechnet die Summe der Gewichtungen für die Datensätze, die dieselbe Kombination von DNS-Namen und -Typ aufweisen. Route 53 beantwortet dann Abfragen, die auf dem Verhältnis der Gewichtung einer Ressource zur Gesamtmenge basieren.

Sie können keine nicht gewichteten Datensätze erstellen, die über dieselben Werte wie gewichtete Datensätze für Datensatzname und Datensatztyp verfügen.

Geben Sie eine Ganzzahl zwischen 0 und 255 ein. Zum Deaktivieren der Weiterleitung an eine Ressource setzen Sie für Weight (Gewichtung) den Wert 0 fest. Wenn Sie Weight (Gewichtung) für alle Datensätze in der Gruppe auf 0 setzen, wird der Datenverkehr mit gleicher Wahrscheinlichkeit zu allen Ressourcen weitergeleitet. Auf diese Weise wird verhindert, dass Sie die Weiterleitung für eine Gruppe von gewichteten Datensätzen versehentlich deaktivieren.

Wenn Sie Zustandsprüfungen mit gewichteten Datensätzen verknüpfen und Weight (Gewichtung) auf 0 setzen, unterscheidet sich das Resultat. Weitere Informationen finden Sie unter So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind.

Gesundheitscheck

Wählen Sie eine Zustandsprüfung aus, wenn Route 53 den Status eines angegebenen Endpunkts überprüfen und DNS-Abfragen mit diesem Eintrag nur beantworten soll, wenn der Endpunkt fehlerfrei ist.

Route 53 prüft den Zustand des im Datensatz angegebenen Endpunkts nicht, z. B. des durch die IP-Adresse im Feld Wert definierten Endpunkts. Wenn Sie eine Zustandsprüfung für einen Datensatz auswählen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Informationen dazu, wie Route 53 ermittelt, ob ein Endpunkt fehlerfrei ist, finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Die Verknüpfung einer Zustandsprüfung mit einem Datensatz ist nur nützlich, wenn Route 53 zwischen mindestens zwei Datensätzen auswählt, um auf eine DNS-Abfrage zu antworten, und Route 53 die Auswahl zum Teil anhand des Status einer Zustandsprüfung treffen soll. Verwenden Sie Zustandsprüfungen nur in den folgenden Konfigurationen:

- Sie überprüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen, die denselben Namen, denselben Typ und dieselbe Routing-Richtlinie haben (z. B. Failover oder gewichtete Datensätze), und Sie geben eine Integritätsprüfung IDs für alle Datensätze an. Wenn die Zustandsprüfung für einen Datensatz einen Endpunkt angibt, der nicht fehlerfrei ist, antwortet Route 53 nicht mehr auf Abfragen, die den Wert für diesen Datensatz verwenden.
- Sie wählen Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) für einen Alias-Datensatz oder die Datensätze in einer Gruppe aus Failover-Alias-, Geolocation-Alias-, Latenz-Alias-, IP-basierten Alias- oder gewichteten Alias-Datensätzen aus. Wenn die Alias-Datensätze andere als Alias-Datensätze in derselben gehosteten Zone referenzieren, müssen Sie auch Zustandsprüfungen für die referenzierten Datensätze angeben. Wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und Yes (Ja) für Evaluate Target Health (Zustand des Ziels bewerten) auswählen, müssen beide mit „True“ ausgewertet werden. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

Wenn Ihre Zustandsprüfungen den Endpunkt nur nach Domainname angeben, sollten Sie für jeden Endpunkt eine eigene Zustandsprüfung erstellen. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Sie müssen in Domain Name (Domänenname) als Wert den Domänennamen des Servers angeben (z. B. us-east-2-www.example.com), nicht den Namen der Datensätze (example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Evaluate Target Health

Wählen Sie Ja aus, wenn Route 53 ermitteln soll, ob auf DNS-Abfragen, die diesen Datensatz verwenden, geantwortet werden soll, indem der Zustand der in Endpunkt angegebenen Ressource geprüft wird.

Beachten Sie Folgendes:

API Gateway, kundenspezifisch, regional APIs und Edge-optimiert APIs

Es gibt keine besonderen Anforderungen für das Festlegen von Evaluate target health (Zielzustand bewerten) auf Yes (Ja), wenn der Endpunkt eine benutzerdefinierte regionale API-Gateway-API oder eine Edge-optimierte API ist.

CloudFront Verteilungen

Sie können die Option Zielintegrität bewerten nicht auf Ja setzen, wenn es sich bei dem Endpunkt um eine CloudFront Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpoint eine Elastic Beanstalk Beanstalk-Umgebung angeben und die Umgebung einen ELB-Load Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine EC2 Amazon-Instance umfasst.) Wenn Sie Evaluate target health auf Ja setzen und entweder keine EC2 Amazon-Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere verfügbare Ressourcen weiter, die fehlerfrei sind, falls vorhanden.

Wenn die Umgebung eine einzelne EC2 Amazon-Instance enthält, gibt es keine besonderen Anforderungen.

ELB-Load Balancer

Das Verhalten der Zustandsprüfung ist abhängig vom Typ des Load Balancers:

- Classic Load Balancers — Wenn Sie einen ELB Classic Load Balancer in Endpoint angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien EC2 Amazon-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Evaluate Target Health auf Ja setzen und entweder keine EC2 Instances fehlerfrei sind oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere Ressourcen weiter.
- Anwendung und Network Load Balancer – Wenn Sie eine ELB-Anwendung oder einen Network Load Balancer angeben und Zielzustand bewerten auf Ja festlegen, leitet Route 53 Abfragen basierend auf dem Zustand der mit dem Load Balancer verknüpften Zielgruppen an den Load Balancer weiter:
  - Damit ein Application oder Network Load Balancer als fehlerfrei gilt, muss jede Zielgruppe mit Zielen mindestens ein fehlerfreies Ziel enthalten. Falls eine Zielgruppe nur fehlerhafte Ziele enthält, gilt der Load Balancer als fehlerhaft und Route 53 leitet Abfragen an andere Ressourcen weiter.
  - Eine Zielgruppe ohne registrierte Ziele gilt als fehlerhaft.

> **Note**
>
> Beim Erstellen eines Load Balancers konfigurieren Sie Einstellungen für Elastic Load Balancing-Zustandsprüfungen. Dies sind keine Route 53-Zustandsprüfungen. Sie erfüllen aber eine ähnliche Funktion. Erstellen Sie keine Route 53-Zustandsprüfungen für die EC2 Instances, die Sie bei einem ELB-Load Balancer registrieren.

S3-Buckets

Es gibt keine speziellen Anforderungen, nach denen Evaluate Target Health (Zielzustand bewerten) auf Yes (Ja) festgelegt werden muss, wenn es sich beim Endpunkt um einen S3-Bucket handelt.

Amazon-VPC-Schnittstellenendpunkte

Es gibt keine besonderen Anforderungen für das Festlegen der Zielzustand bewerten auf Ja, wenn der Endpunkt ein Amazon-VPC-Schnittstellenendpunkt ist.

Andere Datensätze innerhalb derselben gehosteten Zone

Wenn es sich bei der AWS Ressource, die Sie in Endpoint angeben, um einen Datensatz oder eine Gruppe von Datensätzen (z. B. um eine Gruppe gewichteter Datensätze) handelt, es sich jedoch nicht um einen weiteren Alias-Datensatz handelt, empfehlen wir, allen Datensätzen

im Endpunkt eine Integritätsprüfung zuzuordnen. Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe von gewichteten Datensätzen eindeutig identifiziert.

Erstellen von Datensätzen durch Importieren einer Zonendatei

Wenn Sie eine Migration von einem anderen DNS-Serviceanbieter durchführen und dieser DNS-Serviceanbieter Sie die aktuellen DNS-Einstellungen in eine Zonendatei exportieren lässt, können Sie schnell alle Datensätze für eine gehostete Amazon-Route-53-Zone erstellen, indem Sie eine Zonendatei importieren.

> **Note**
>
> Eine Zonendatei verwendet ein Standardformat namens BIND zur Darstellung von Datensätzen in einem Textformat. Informationen zum Format einer Zonendatei finden Sie im Wikipedia-Eintrag Zonendatei. Weitere Informationen finden Sie in Abschnitt 3.6.1 von RFC 1034, Domain Names—Concepts and Facilities und in Abschnitt 5 von RFC 1035, Domain Names—Implementation and Specification.

Beachten Sie Folgendes, wenn Sie Datensätze durch Importieren einer Zonendatei erstellen möchten:

- Die Zonendatei muss in einem RFC-konformen Format sein.
- Der Domainname jedes Datensatzes in einer gehosteten Zone muss mit dem Namen der gehosteten Zone enden.
- Route 53 unterstützt die `$ORIGIN`- und `$TTL`-Schlüsselwörter. Wenn die Zonendatei `$GENERATE` oder `$INCLUDE`-Schlüsselwörter enthält, schlägt der Import fehl und Route 53 gibt einen Fehler zurück.
- Wenn Sie die Zonendatei importieren, ignoriert Route 53 den SOA-Datensatz in der Zonendatei. Route 53 ignoriert auch alle NS-Datensätze, die denselben Namen haben wie die gehostete Zone.
- Sie können maximal 1000 Datensätze importieren.

- Wenn die gehostete Zone bereits Datensätze enthält, die in der Zonendatei angezeigt werden, schlägt der Importvorgang fehl und es werden keine Datensätze erstellt.
- Bei TXT-Datensätzen, die Backslash-Zeichen enthalten, interpretiert der Import der Zonendatei bestimmte Backslash-Sequenzen als Steuerzeichen. Um wörtliche Backslash-Zeichen in TXT-Datensatzwerte aufzunehmen:
  - Verwenden Sie doppelte Backslashes (`\\\\`) in der Zonendatei, um einen einzelnen buchstäblichen Backslash im endgültigen TXT-Datensatz darzustellen.
  - Wenn Ihr TXT-Eintrag beispielsweise `\\jYTDWqH...` (mit einem buchstäblichen Backslash und j) enthalten soll, geben Sie dies in der Zonendatei an. `\\\\jYTDWqH...`

  Dies ist besonders wichtig für ACME-Challenge-Datensätze und andere TXT-Datensätze, die buchstäbliche Backslash-Zeichen enthalten.
- Bei langen TXT-Datensätzen (wie DKIM-Datensätzen) unterstützt der Importvorgang für Zonendateien die Aufteilung des Inhalts in mehrere Zeichenfolgen. Um TXT-Einträge mit mehreren Zeichenketten zu erstellen:
  - Verwenden Sie separate Zeilen in Ihrer Zonendatei mit demselben Datensatznamen und -typ.

    Example

    ```
    example.com. 300 IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC"
    example.com. 300 IN TXT
     "7fCC6C13dM9tXuJmUBH7D4Vw8y1ByJ8z9QX2fvLm3pN4sR5tU6vW7xY8zA9bC0dE1f"
    example.com. 300 IN TXT
     "G2hI3jK4lM5nO6pQ7rS8tU9vW0xY1zA2bC3dE4fG5hI6jK7lM8nO9pQ0rS1tU2vW3x"
    ```

  Der Importvorgang kombiniert diese automatisch zu einem einzigen TXT-Datensatz mit mehreren Zeichenfolgen. Jede einzelne Zeichenfolge kann bis zu 65.535 Zeichen enthalten. Verketten Sie lange Zeichenketten nicht zu einem einzigen Wert in Anführungszeichen.
- Wir empfehlen, dass Sie den Inhalt der Zonendatei überprüfen, um zu bestätigen, dass Datensatznamen gegebenenfalls einen abschließenden Punkt enthalten oder ausschließen:
  - Wenn der Name eines Datensatzes in der Zonendatei einen abschließenden Punkt enthält (`example.com.`), interpretiert der Importprozess den Namen als voll qualifizierten Domainnamen und erstellt einen Route-53-Datensatz mit diesem Namen.
  - Wenn der Name eines Datensatz in der Zonendatei keinen abschließenden Punkt enthält (`www`), verbindet der Importprozess diesen Namen mit dem Domainnamen in der Zonendatei

(`example.com`) und erstellt einen Route-53-Datensatz mit diesem zusammengefügten Namen (`www.example.com`).

Wenn der Exportprozess keinen abschließenden Punkt zu den vollqualifizierten Domainnamen eines Datensatzes hinzufügt, fügt der Route-53-Importprozess den Domainnamen zum Namen des Datensatzes hinzu. Nehmen wir beispielsweise an, dass Sie Datensätze in die gehostete Zone `example.com` importieren und der Name eines MX-Datensatzes in dieser Zonendatei `mail.example.com` (ohne abschließenden Punkt) ist. Der Route-53-Importprozess erstellt einen MX-Datensatz mit dem Namen `mail.example.com.example.com`.

> **Important**
>
> Für CNAME-, MX-, PTR- und SRV-Datensätze gilt dieses Verhalten auch für den Domainnamen, der im RDATA-Wert enthalten ist. Nehmen wir beispielsweise an, dass Sie eine Zonendatei für `example.com` haben. Wenn ein CNAME-Datensatz in der Zonendatei (`support`, ohne abschließenden Punkt) den RDATA-Wert `www.example.com` (auch ohne abschließenden Punkt) hat, erstellt der Importprozess einen Route-53-Datensatz mit dem Namen `support.example.com`, der Datenverkehr an `www.example.com.example.com` weiterleitet. Überprüfen Sie die RDATA-Werte und aktualisieren Sie sie entsprechend, bevor Sie Ihre Zonendatei importieren. Verwenden Sie bei TXT-Datensätzen, die Backslash-Zeichen enthalten, doppelte Backslashes (\\\\) in der Zonendatei, um wörtliche Backslashes darzustellen.

Route 53 unterstützt das Exportieren von Datensätzen in eine Zonendatei nicht.

> **Note**
>
> Wenn Sie einen Datensatz erstellen, der denselben Namen wie die gehostete Zone hat, geben Sie im Feld Name keinen Wert ein (zum Beispiel ein @-Symbol).

So erstellen Sie Datensätze durch den Import einer Zonendatei:

1. Sichern Sie sich eine Zonendatei vom DNS-Serviceanbieter, der aktuell den Service für die Domain bereitstellt. Der Prozess und die Terminologie unterscheiden sich von einem Anbieter zum nächsten. Sehen Sie sich die Schnittstelle und Dokumentation Ihres Anbieters an, um

Informationen zum Exportieren und Speichern Ihrer Datensätze in einer Zonendatei oder BIND-Datei zu erhalten.

Wenn der Prozess komplizierter ist, bitten Sie den Kundendienst Ihres aktuellen DNS-Anbieters um Ihre Datensatzliste oder Zonendatei-Informationen.

2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Erstellen Sie auf der Seite Hosted Zones (Gehostete Zonen) eine neue gehostete Zone:
   a. Wählen Sie Create hosted zone (Erstellte gehostete Zone).
   b. Geben Sie den Namen Ihrer Domain und optional eine Anmerkung ein.
   c. Wählen Sie Erstellen aus.
5. Wählen Sie Import Zone File (Zonendatei importieren).
6. Fügen Sie im Bereich Import Zone File (Zonen-Datei importieren) die Inhalte Ihrer Zonendatei in das Textfeld Zone File (Zonendatei) ein.
7. Wählen Sie Importieren aus.

> **Note**
>
> Abhängig von der Anzahl der Datensätze in Ihrer Zonendatei müssen Sie möglicherweise einige Minuten warten, bis die Datensätze erstellt sind.

8. Wenn Sie einen anderen DNS-Service für die Domain verwenden (was üblich ist, wenn Sie Ihre Domain bei einer anderen Vergabestelle registriert haben), können Sie den DNS-Service zu Route 53 migrieren. Wenn dieser Schritt abgeschlossen ist, erkennt Ihre Vergabestelle Route 53 als Ihren DNS-Service bei DNS-Abfragen für Ihre Domain und die Abfragen werden an Route-53-DNS-Server gesendet. (In der Regel dauert es ein oder zwei Tage, bis DNS-Abfragen zu Route 53 geleitet werden, weil die Informationen zu Ihrem vorherigen DNS-Service so lange im Cache von DNS-Resolvern abgelegt sind.) Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Bearbeiten von Datensätzen

Im folgenden Verfahren wird das Bearbeiten von Datensätzen mit der Amazon-Route-53-Konsole erläutert. Informationen zum Bearbeiten von Datensätzen mithilfe der Route 53-API finden Sie ChangeResourceRecordSetsin der Amazon Route 53-API-Referenz.

> **Note**
>
> Die Verteilung der Änderungen an Ihren neuen Datensätzen auf die Route 53-DNS-Server nimmt etwas Zeit in Anspruch. Derzeit besteht die einzige Möglichkeit, um zu überprüfen, ob Änderungen weitergegeben wurden, darin, die GetChangeAPI-Aktion zu verwenden. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

So bearbeiten Sie Datensätze mithilfe der Route-53-Konsole:

1. Wenn Sie keine Alias-Datensätze bearbeiten, fahren Sie mit Schritt 2 fort.

   Wenn Sie Alias-Datensätze bearbeiten, die Datenverkehr an einen Classic Load Balancer mit Elastic Load Balancing, an einen Application Load Balancer oder an einen Network Load Balancer weiterleiten, und Sie Ihre gehostete Route-53-Zone und Ihren Load Balancer mit verschiedenen Konten erstellt haben, befolgen Sie die Schritte im Verfahren Abrufen des DNS-Namens für einen Elastic Load Balancing Load Balancer, um den DNS-Namen für den Load Balancer abzurufen.

   Wenn Sie Aliaseinträge für eine andere AWS Ressource bearbeiten, fahren Sie mit Schritt 2 fort.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) die Zeile der gehosteten Zone, die die zu löschenden Datensätze enthält.
5. Wählen Sie die Zeile für den Datensatz aus, den Sie bearbeiten möchten und geben Sie Ihre Änderungen im Bereich Edit record (Bearbeiten von Datensätzen) ein.
6. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Amazon Route 53-Datensätzen angeben.
7. Wählen Sie Änderungen speichern aus.

8. Wenn Sie mehrere Datensätze bearbeiten, wiederholen Sie die Schritte 5 bis 7.

Löschen von Datensätzen

Im folgenden Verfahren wird das Löschen von Datensätzen mit der Route-53-Konsole erläutert. Informationen zum Löschen von Datensätzen mithilfe der Route 53-API finden Sie ChangeResourceRecordSetsin der Amazon Route 53-API-Referenz.

> **Note**
>
> Die Verteilung der Änderungen an Ihren neuen Datensätzen auf die Route 53-DNS-Server nimmt etwas Zeit in Anspruch. Derzeit besteht die einzige Möglichkeit, um zu überprüfen, ob Änderungen weitergegeben wurden, darin, die GetChangeAPI-Aktion zu verwenden. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

So löschen Sie Datensätze:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie auf der Seite „Gehostete Zonen“ die Zeile der gehosteten Zone, die die zu löschenden Datensätze enthält.
3. Wählen Sie in der Liste der Datensatzsätze den Datensatz aus, den Sie löschen möchten.

   Um mehrere aufeinander folgende Datensätze auszuwählen, wählen Sie die erste Zeile, halten Sie die Umschalttaste gedrückt und klicken Sie dann auf die letzte Zeile. Um mehrere nicht aufeinanderfolgende Datensätze auszuwählen, wählen Sie die erste Zeile, halten Sie die Steuerungstaste gedrückt und wählen Sie dann weitere Zeilen.

   Sie können keine Datensätze löschen, die über einen Wert von NS oder SOA für Type (Typ) verfügen.
4. Wählen Sie Löschen aus.
5. Wählen Sie Löschen, um das Dialogfeld zu schließen.

Auflisten von Datensätzen

Im folgenden Verfahren wird das Auflisten der Datensätze in einer gehosteten Zone mithilfe der Amazon-Route-53-Konsole erläutert. Informationen zum Auflisten von Datensätzen mithilfe der Route 53-API finden Sie ListResourceRecordSetsin der Amazon Route 53-API-Referenz.

So listen Sie Datensätze auf:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) den Namen der gehosteten Zone aus.
4. Um den Suchmodus zu ändern, wählen Sie das Zahnradsymbol oben rechts in der Tabelle Datensätze. Wählen Sie eine der folgenden Optionen:

   - Automatisch

     In diesem Modus verwendet der Service einen Filter auf der Grundlage einer Anzahl von Datensätzen. Voll bei weniger als 2 000 und schnell bei mehr als 2 000 Datensätzen.

   - Voll

     In diesem Modus sind alle Suchfilter verfügbar, aber die Suchleistung kann langsamer sein.

   - Schnell

     In diesem Modus sind einige erweiterte Features nicht verfügbar, aber die Suchleistung ist schneller.

Um nur ausgewählte Datensätze anzuzeigen, geben Sie die entsprechenden Suchkriterien über der Liste der Datensätze ein. Im automatischen Modus hängt das Suchverhalten davon ab, ob die gehostete Zone bis zu 2 000 Datensätze oder mehr als 2 000 Datensätze enthält:

Bis zu 2 000 Datensätze und Vollmodus

- Um die Datensätze mit bestimmten Werten anzuzeigen, geben Sie einen Wert in die Suchleiste ein und drücken Sie die Eingabetaste. Wenn Sie beispielsweise die Datensätze anzeigen möchten, die eine IP-Adresse haben, die mit 192.0 beginnt, geben Sie diesen Wert in das Feld Search (Suche) ein, und drücken Sie Enter (Eingabetaste).

- Um nur die Datensätze anzuzeigen, die denselben DNS-Datensatztyp aufweisen, wählen Sie Datensatztyp in der Dropdown-Liste und geben Sie den Datensatztyp ein.
- Um nur Alias-Datensätze anzuzeigen, wählen Sie Aliasnamen in der Dropdown-Liste und geben Sie **`Yes`** ein.
- Um nur gewichtete Datensätze anzuzeigen, wählen Sie Routing-Richtlinie in der Dropdown-Liste und geben Sie **`WEIGHTED`** ein.

Mehr als 2 000 Datensätze und Schnellmodus

- Sie können nun nach Datensatznamen, nicht nach Datensatzwerten suchen lassen. Es ist auch nicht möglich, die Datensätze nach Typ oder nach Alias- oder gewichteten Datensätzen zu filtern.

  Platzieren Sie dazu den Cursor im Textfeld Filter und wählen Sie Eigenschaften **>** Datensatzname aus.
- Für Datensätze mit drei Bezeichnungen (drei durch Punkte voneinander getrennten Teilen) gilt: Wenn Sie einen Wert in das Suchfeld eingeben und die Eingabetaste drücken, führt die Route-53-Konsole automatisch eine Platzhaltersuche für die dritte Bezeichnung von rechts im Datensatznamen durch. Nehmen wir beispielsweise an, die gehostete Zone example.com enthält 100 Datensätze mit der Bezeichnung record1.example.com bis record100.example.com. (Record1 ist die dritte Bezeichnung von rechts.) Dies geschieht, wenn Sie eine Suche nach den folgenden Werten durchführen:
  - record1 – Die Route-53-Konsole sucht nach record1*.example.com, wobei record1.example.com, record10.example.com bis record19.example.com und record100.example.com zurückgegeben werden.
  - record1.example.com – Wie im vorherigen Beispiel sucht die Konsole nach record1*.example.com und es werden die gleichen Datensätze zurückgegeben.
  - 1 – Die Konsole sucht nach 1*.example.com und es werden keine Datensätze zurückgegeben.
  - example – Die Konsole sucht nach example*.example.com und es werden keine Datensätze zurückgegeben.
  - example.com – In diesem Beispiel führt die Konsole keine Platzhaltersuche durch. Es werden alle Datensätze in der gehosteten Zone zurückgegeben.
  - Automatischer Suchmodus: Bei Verwendung dieses Suchmodus müssen Sie zuerst eine Eigenschaft wie etwa den Datensatznamen angeben, um suchen zu können.

> **Note**
>
> Wenn die dritte Bezeichnung von rechts mindestens einen Bindestrich enthält (z. B. `third-label.example.com`) und Sie nach dem Teil der dritten Bezeichnung unmittelbar vor dem Bindestrich suchen (`third` in diesem Beispiel), gibt Route 53 keine Datensätze zurück. Stattdessen sollten Sie entweder den Bindestrich einschließen (nach `third-` suchen) oder das Zeichen unmittelbar vor dem Bindestrich weglassen (nach `third` suchen).

- Bei Datensätzen, die vier oder mehr Bezeichnungen haben, müssen Sie den genauen Namen des Datensatzes angeben. Platzhaltersuchen werden nicht unterstützt. Wenn z. B. die gehostete Zone einen Datensatz mit dem Namen label4.record1.example.com enthält, finden Sie diesen Datensatz nur dann, wenn Sie label4.record1.example.com in das Suchfeld eingeben.

Konfigurieren der DNSSEC-Signatur in Amazon Route 53

DNSSEC-Signatur (Domain Name System Security Extensions) ermöglicht DNS-Resolvern zu überprüfen, ob eine DNS-Antwort von Amazon Route 53 stammt und nicht manipuliert wurde. Wenn Sie die DNSSEC-Signatur verwenden, wird jede Antwort für eine gehostete Zone mithilfe der Kryptografie mit öffentlichen Schlüsseln signiert. Einen Überblick über DNSSEC finden Sie im Abschnitt DNSSEC von AWS re:Invent 2021 — Amazon Route 53: Ein Jahr im Rückblick.

In diesem Kapitel erklären wir, wie Sie die DNSSEC-Signatur für Route 53 aktivieren, wie Sie mit Schlüsselsignaturschlüsseln () arbeiten und wie Sie Probleme beheben können. KSKs Sie können mit der DNSSEC-Signatur in der oder programmgesteuert mit der AWS-Managementkonsole API arbeiten. Weitere Informationen zur Verwendung der CLI oder SDKs zur Arbeit mit Route 53 finden Sie unterAmazon Route 53 einrichten.

Bevor Sie DNSSEC-Signatur aktivieren, beachten Sie Folgendes:

- Um einen Zonenausfall zu verhindern und Probleme mit der Nichtverfügbarkeit Ihrer Domäne zu vermeiden, müssen Sie DNSSEC-Fehler schnell beheben und beheben. Es wird dringend empfohlen, einen CloudWatch Alarm einzurichten, der Sie benachrichtigt, wenn ein `DNSSECInternalFailure` `DNSSECKeySigningKeysNeedingAction` Oder-Fehler erkannt wird. Weitere Informationen finden Sie unter Überwachung von Hosting-Zonen mit Amazon CloudWatch.

- Es gibt zwei Arten von Schlüsseln in DNSSEC: einen Schlüssel-Signaturschlüssel (KSK) und einen Zonen-Signaturschlüssel (ZSK). Bei der DNSSEC-Signierung von Route 53 basiert jede KSK auf einemAsymmetrische kundenverwaltete Schlüsselin AWS KMS dass Sie besitzen. Sie sind für das Management von KSK verantwortlich, was bei Bedarf auch das Drehen beinhaltet. Das ZSK-Management wird von der Route 53 durchgeführt.
- Wenn Sie DNSSEC-Signierung für eine gehostete Zone aktivieren, begrenzt Route 53 die TTL auf eine Woche. Wenn Sie eine TTL von mehr als einer Woche für Datensätze in der gehosteten Zone festlegen, wird keine Fehlermeldung angezeigt. Route 53 erzwingt jedoch eine TTL von einer Woche für die Datensätze. Datensätze mit einer TTL von weniger als einer Woche und Datensätze in anderen gehosteten Zonen, für die keine DNSSEC-Signatur aktiviert ist, sind nicht betroffen.
- Wenn Sie DNSSEC-Signatur verwenden, werden Konfigurationen verschiedener Anbieter nicht unterstützt. Wenn Sie White-Label-Nameserver (auch bekannt als Vanity-Nameserver oder Private-Nameserver) konfiguriert haben, stellen Sie sicher, dass diese Nameserver von einem einzigen DNS-Anbieter bereitgestellt werden.
- Einige DNS-Anbieter unterstützen keine Delegation Signer (DS) -Einträge in ihrem autorisierenden DNS. Wenn Ihre übergeordnete Zone von einem DNS-Anbieter gehostet wird, der keine DS-Abfragen unterstützt (kein AA-Flag in der DS-Abfrageantwort setzt), kann die untergeordnete Zone nicht mehr aufgelöst werden, wenn Sie DNSSEC in seiner untergeordneten Zone aktivieren. Stellen Sie sicher, dass Ihr DNS-Anbieter DS-Einträge unterstützt.
- Es kann hilfreich sein, IAM-Berechtigungen einzurichten, damit ein anderer Benutzer neben dem Zonenbesitzer Datensätze in der Zone hinzufügen oder entfernen kann. Ein Zonenbesitzer kann beispielsweise eine KSK hinzufügen und die Signatur aktivieren und möglicherweise auch für die Schlüsselrotation verantwortlich sein. Möglicherweise ist eine andere Person jedoch für die Arbeit mit anderen Datensätzen für die gehostete Zone verantwortlich. Eine IAM-Beispielrichtlinie finden Sie unter Beispielberechtigungen für einen Domänendatensatzbesitzer.
- Informationen darüber, ob die TLD DNSSEC-Unterstützung bietet, finden Sie unter. Domains, die Sie mit Amazon Route 53 registrieren können

Themen

- Aktivieren der DNSSEC-Signierung und Aufbau einer Vertrauenskette
- Deaktivieren der DNSSEC-Signatur
- Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC
- Arbeiten mit Schlüsseln zur Schlüsselsignierung () KSKs
- KMS-Schlüssel- und ZSK-Verwaltung in Route 53

- DNSSEC-Nachweise für Nichtvorhandensein in Route 53
- Fehlerbehebung für DNSSEC

Aktivieren der DNSSEC-Signierung und Aufbau einer Vertrauenskette

Die inkrementellen Schritte gelten für den Besitzer der gehosteten Zone und den übergeordneten Zonenbetreuer. Dies kann dieselbe Person sein, aber falls nicht, sollte der Zonenbesitzer den übergeordneten Zonenbetreuer benachrichtigen und mit ihm arbeiten.

Wir empfehlen, die Schritte in diesem Artikel zu befolgen, damit Ihre Zone signiert und in die Vertrauenskette aufgenommen wird. Die folgenden Schritte minimieren das Risiko des Onboardings auf DNSSEC.

> **Note**
>
> Stellen Sie sicher, dass Sie die Voraussetzungen lesen, bevor Sie in Konfigurieren der DNSSEC-Signatur in Amazon Route 53 beginnen.

Es müssen drei Schritte durchgeführt werden, um die DNSSEC-Signatur zu aktivieren, indem Sie wie in den folgenden Abschnitten beschrieben vorgehen.

Themen

- Schritt 1: Vorbereiten der Aktivierung der DNSSEC-Signatur
- Schritt 2: Aktivieren der DNSSEC-Signatur und Erstellen einer KSK
- Schritt 3: Erstellen einer Vertrauenskette

Schritt 1: Vorbereiten der Aktivierung der DNSSEC-Signatur

Die Vorbereitungsschritte helfen Ihnen, das Risiko eines Onboardings bei DNSSEC zu minimieren, indem Sie die Zonenverfügbarkeit überwachen und die Wartezeiten zwischen dem Aktivieren der Signierung und dem Einfügen des Delegation Signer (DS)-Datensatzes senken.

So bereiten Sie sich auf das Aktivieren der DNSSEC-Signierung vor

1. Überwachen Sie die Verfügbarkeit der Zone.

Sie können die Zone auf die Verfügbarkeit Ihrer Domänennamen überwachen. Dies kann Ihnen helfen, alle Probleme zu beheben, die einen Schritt zurücksetzen könnten, nachdem Sie die DNSSEC-Signatur aktiviert haben. Sie können Ihre Domänennamen mit dem größten Datenverkehr überwachen, indem Sie die Abfrageprotokollierung verwenden. Für weitere Informationen zum Einrichten einer Abfrage-Protokollierung siehe Amazon Route 53 überwachen.

Die Überwachung kann über ein Shell-Skript oder über einen Drittanbieterdienst erfolgen. Dies sollte jedoch nicht das einzige Signal sein, um festzustellen, ob ein Rollback erforderlich ist. Möglicherweise erhalten Sie auch Feedback von Ihren Kunden, da eine Domäne nicht verfügbar ist.

2. Senken Sie die maximale TTL der Zone.

   Die maximale TTL der Zone ist der längste TTL-Datensatz in der Zone. In der folgenden Beispielzone beträgt die maximale TTL der Zone 1 Tag (86 400 Sekunden).

Name	TTL	Datensatz-Klasse	Datensatztyp	Datensatz-Daten
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**

Die Senkung der maximalen TTL der Zone trägt dazu bei, die Wartezeit zwischen dem Aktivieren der Signatur und dem Einfügen des Delegation Signer (DS)-Datensatzes zu verkürzen. Wir empfehlen, die maximale TTL der Zone auf eine Stunde (3 600 Sekunden) zu senken. Auf diese Weise können Sie sie nach nur einer Stunde zurücksetzen, wenn ein Resolver Probleme beim Zwischenspeichern signierter Datensätze hat.

Rollback: Machen Sie die TTL-Änderungen rückgängig.

3. Senken Sie das SOA-TTL- und SOA-Mindestfeld.

   Das SOA-Mindestfeld ist das letzte Feld in den SOA-Datensatzdaten. Im folgenden SOA-Beispieldatensatz hat das Mindestfeld den Wert 5 Minuten (300 Sekunden).

Name	TTL	Datensatz-Klasse	Datensatztyp	Datensatz-Daten
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 2002022401 10800 15 604800 300

   Das SOA-TTL- und SOA-Mindestfeld bestimmt, wie lange Resolver sich an negative Antworten erinnern. Nachdem Sie die Signierung aktiviert haben, geben die Nameserver der Route 53 NSEC-Datensätze für negative Antworten zurück. Die NSEC enthält Informationen, die Resolver verwenden könnten, um eine negative Antwort zu synthetisieren. Wenn Sie ein Rollback durchführen müssen, weil die NSEC-Informationen dazu geführt haben, dass ein Resolver eine negative Antwort für einen Namen annimmt, müssen Sie nur auf das Maximum des SOA-TTL- und SOA-Mindestfeldes warten, damit der Resolver die Annahme stoppt.

   Rollback: Machen Sie die SOA-Änderungen rückgängig.

4. Stellen Sie sicher, dass die Änderungen an den Mindestfeldern TTL und SOA wirksam sind.

Verwenden Sie diese GetChangeOption, um sicherzustellen, dass Ihre bisherigen Änderungen an alle Route 53-DNS-Server weitergegeben wurden.

Schritt 2: Aktivieren der DNSSEC-Signatur und Erstellen einer KSK

Sie können die DNSSEC-Signatur aktivieren und einen Schlüsselsignierungsschlüssel (KSK) erstellen, indem Sie AWS CLI oder die Route 53-Konsole verwenden.

- CLI
- Konsole

Wenn Sie einen KMS-Schlüssel bereitstellen oder erstellen, gibt es mehrere Anforderungen. Weitere Informationen finden Sie unter Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC.

CLI

Sie können einen Schlüssel verwenden, den Sie bereits zur Verfügung haben, oder Sie erstellen einen, indem Sie einen AWS CLI -Befehl wie den folgenden mit eigenen Werten für `hostedzone_id`, `cmk_arn`, `ksk_name`, und `unique_string` (um die Anfrage eindeutig zu machen) verwenden:

```
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
```

Weitere Informationen zu den vom Kunden verwalteten Schlüsseln finden Sie unter Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC. Siehe auch CreateKeySigningKey.

Um die DNSSEC-Signatur zu aktivieren, führen Sie einen AWS CLI Befehl wie den folgenden aus und verwenden Sie dabei Ihren eigenen Wert für: `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

Weitere Informationen finden Sie unter enable-hosted-zone-dnssecund EnableHostedZone DNSSEC.

Console

So aktivieren Sie die DNSSEC-Signatur und erstellen eine KSK

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im NavigationsbereichGehostete ZonenWählen Sie dann eine gehostete Zone aus, für die Sie die DNSSEC-Signatur aktivieren möchten.
3. Klicken Sie auf derDNSSECWählen Sie auf der RegisterkarteDNSSEC-Signatur aktivierenaus.

   > **Note**
   >
   > Wenn die Option in diesem AbschnittDNSSEC-Signatur deaktivierenDer erste Schritt zur Aktivierung der DNSSEC-Signatur ist bereits abgeschlossen. Stellen Sie sicher, dass Sie eine Vertrauenskette für die gehostete Zone für DNSSEC einrichten oder bereits vorhanden sind, und Sie sind fertig. Weitere Informationen finden Sie unter Schritt 3: Erstellen einer Vertrauenskette.

4. Wählen Sie im Abschnitt Schlüsselsignaturschlüsselerstellung (KSK) Create new KSK (Neuen KSK erstellen), aus und geben Sie unter Provide KSK name (KSK-Namen angeben) einen Namen für den KSK ein, den Route 53 für Sie erstellen wird. Namen können nur Buchstaben, Zahlen und Unterstriche enthalten. Dieser Wert muss eindeutig sein.
5. UNDERKundenverwalteter CMKden vom Kunden verwalteten Schlüssel für Route 53 aus, der beim Erstellen des KSK für Sie verwendet werden soll. Sie können einen vorhandenen vom Kunden verwalteten Schlüssel verwenden, der für die DNSSEC-Signatur gilt, oder einen neuen, vom Kunden verwalteten Schlüssel erstellen.

   Wenn Sie einen vom Kunden verwalteten Schlüssel bereitstellen oder erstellen, gibt es mehrere Anforderungen. Weitere Informationen finden Sie unter Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC.
6. Geben Sie den Alias für einen vorhandenen, vom Kunden verwalteten Schlüssel ein. Wenn Sie einen neuen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie einen Alias für einen vom Kunden verwalteten Schlüssel ein, und Route 53 erstellt einen für Sie.

> **Note**
>
> Wenn Sie sich dafür entscheiden, dass Route 53 einen vom Kunden verwalteten Schlüssel erstellt, beachten Sie, dass für jeden vom Kunden verwalteten Schlüssel separate Gebühren anfallen. Weitere Informationen finden Sie unter AWS Key Management Service – Preise.

7. Klicken Sie auf DNSSEC-Signatur aktivieren.

Führen Sie nach dem Aktivieren der Zonensignierung die folgenden Schritte aus (egal, ob Sie die Konsole oder CLI verwendet haben):

1. Stellen Sie sicher, dass die Zonensignatur effektiv ist.

   Falls Sie dies getan haben AWS CLI, können Sie die Vorgangs-ID aus der Ausgabe des `EnableHostedZoneDNSSEC()` Aufrufs verwenden, um get-change auszuführen oder GetChangeum sicherzustellen, dass alle Route 53-DNS-Server Antworten signieren (Status `=INSYNC`).

2. Warten Sie mindestens auf die maximale TTL der vorherigen Zone.

   Warten Sie, bis Resolver alle nicht signierten Datensätze aus ihrem Cache leeren. Um dies zu erreichen, sollten Sie mindestens auf die maximale TTL der vorherigen Zone warten. In der `example.com`-Zone oben beträgt Wartezeit 1 Tag.

3. Überwachen Sie Berichte über Kundenprobleme.

   Nachdem Sie die Zonensignierung aktiviert haben, sehen Ihre Kunden möglicherweise Probleme im Zusammenhang mit Netzwerkgeräten und Resolvern. Der empfohlene Überwachungszeitraum beträgt 2 Wochen.

   Im Folgenden finden Sie Beispiele für Probleme, die möglicherweise auftreten:

   - Einige Netzwerkgeräte können die DNS-Antwortgröße auf unter 512 Byte beschränken, was für einige signierte Antworten zu klein ist. Diese Netzwerkgeräte sollten neu konfiguriert werden, um größere DNS-Antwortgrößen zu ermöglichen.
   - Einige Netzwerkgeräte führen eine gründliche Untersuchung der DNS-Antworten durch und entfernen bestimmte Datensätze, die sie nicht verstehen, wie die für DNSSEC verwendeten. Diese Geräte sollten neu konfiguriert werden.

- Die Resolver einiger Kunden behaupten, dass sie eine größere UDP-Antwort akzeptieren können, als ihr Netzwerk unterstützt. Sie können Ihre Netzwerkfähigkeit testen und Ihre Resolver entsprechend konfigurieren. Weitere Informationen finden Sie unter DNS-Antwortgröße-Testserver.

Rollback: Rufen Sie DisableHostedZoneDNSSEC auf und führen Sie dann ein Rollback der Schritte unter durch. Schritt 1: Vorbereiten der Aktivierung der DNSSEC-Signatur

Schritt 3: Erstellen einer Vertrauenskette

Nachdem Sie die DNSSEC-Signatur für eine gehostete Zone in Route 53 aktiviert haben, richten Sie eine Vertrauenskette für die gehostete Zone ein, um die DNSSEC-Signatureinrichtung abzuschließen. Dazu erstellen Sie einen Delegation Signer (DS) -Datensatz imparent-gehostete Zone für Ihre gehostete Zone mit den Informationen, die Route 53 zur Verfügung stellt. Je nachdem, wo Ihre Domain registriert ist, fügen Sie den Datensatz der übergeordneten gehosteten Zone in Route 53 oder bei einer anderen Domänenregistrierungsstelle hinzu.

So richten Sie eine Vertrauenskette für die DNSSEC-Signatur ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im NavigationsbereichGehostete Zonen, und wählen Sie dann eine gehostete Zone aus, für die Sie eine DNSSEC-Vertrauenskette einrichten möchten. Sie müssen zuerst die DNSSEC-Signatur aktivieren.
3. Klicken Sie auf der DNSSEC unter DNSSEC, wählen Sie Anzeigen von Informationen zum Erstellen von DS-Datensätzen aus.

> **Note**
>
> Wenn Sie nicht sehenAnzeigen von Informationen zum Erstellen von DS-Datensätzenin diesem Abschnitt müssen Sie die DNSSEC-Signatur aktivieren, bevor Sie die Vertrauenskette einrichten. Wählen Sie Enable DNSSEC signing (DNSSEC-Signatur aktivieren) aus, führen Sie die unter beschriebenen Schritte in Schritt 2: Aktivieren der DNSSEC-Signatur und Erstellen einer KSK aus und kehren Sie dann zu diesen Schritten zurück, um die Vertrauenskette einzurichten.

4. UNDERErstellen einer Vertrauenskette, wählen Sie entwederRegistrant Route 53oderEine andere Domänenvergabestelle, je nachdem, wo Ihre Domain registriert ist.
5. Verwenden Sie die bereitgestellten Werte ab Schritt 3 , um einen DS-Datensatz für die übergeordnete gehostete Zone in Route 53 zu erstellen. Wenn Ihre Domäne nicht bei Route 53 gehostet wird, verwenden Sie die bereitgestellten Werte, um einen DS-Datensatz auf der Website Ihres Domänen-Registrars zu erstellen.

   Richten Sie eine Vertrauenskette für die übergeordnete Zone ein:

   - Wenn Ihre Domain über Route 53 verwaltet wird, gehen Sie wie folgt vor:

     Stellen Sie sicher, dass Sie den richtigen Signierungsalgorithmus (ECDSAP256SHA256 und Typ 13) und den richtigen Digest-Algorithmus (SHA-256 und Typ 2) konfigurieren.

     Wenn Route 53 Ihr Registrar ist, gehen Sie in der Route-53-Konsole wie folgt vor:

     1. Beachten Sie dieSchlüsseltyp,Signaturalgorithmus, undDer öffentliche Schlüssel-Werte. Klicken Sie im Navigationsbereich auf Registered domains (Registrierte Domänen).
     2. Wählen Sie eine Domain aus und klicken Sie dann auf der Registerkarte DNSSEC-Schlüssel auf Schlüssel hinzufügen.
     3. Wählen Sie im Dialogfeld Manage DNSSEC keys (DNSSEC-Schlüssel verwalten) den entsprechenden Key type (Schlüsseltyp) und Algorithm (Algorithmus) für Route 53 registrar (Route-53-Registrar) aus den Dropdown-Menüs aus.
     4. Kopieren Sie dieDer öffentliche Schlüsselfür den Registrar der Route 53. Wählen Sie in Manage DNSSEC keys (DNSSEC-Schlüssel verwalten) den Wert in dem Feld Public key (Öffentlicher Schlüssel) aus.
     5. Wählen Sie Hinzufügen aus.

        Route 53 fügt den DS-Datensatz der übergeordneten Zone aus dem öffentlichen Schlüssel hinzu. Beispiel: Wenn Ihre Domäne lautet`example.com`Der DS-Eintrag wird der DNS-Zone .com hinzugefügt.

   - Wenn Ihre Domain in einer anderen Registry verwaltet wird, folgen Sie den Anweisungen im Abschnitt Ein anderer Domain-Registrar.

     Um sicherzustellen, dass die folgenden Schritte reibungslos verlaufen, führen Sie eine niedrige DS-TTL in die übergeordnete Zone ein. Wir empfehlen, den DS TTL auf 5 Minuten (300 Sekunden) für eine schnellere Wiederherstellung einzustellen, wenn Sie Ihre Änderungen zurücksetzen müssen.

- Richten Sie eine Vertrauenskette für die untergeordnete Zone ein:

  Wenn Ihre übergeordnete Zone von einer anderen Registrierung verwaltet wird, kontaktieren Sie Ihren Registrar, um den DS-Datensatz für Ihre Zone einzuführen. In der Regel können Sie die TTL des DS-Datensatzes nicht anpassen.

- Wenn Ihre übergeordnete Zone auf Route 53 gehostet wird, kontaktieren Sie den Besitzer der übergeordneten Zone, um den DS-Datensatz für Ihre Zone einzuführen.

  Geben Sie die `$ds_record_value` für den Besitzer der übergeordneten Zone an. Sie können sie abrufen, indem Sie in der Konsole auf Informationen anzeigen klicken, um einen DS-Eintrag zu erstellen, und das DS-Datensatzfeld kopieren, oder indem Sie die GetDNSSec-API aufrufen und den Wert des Felds " abrufen: DSRecord

  ```
  aws --region us-east-1 route53 get-dnssec
              --hosted-zone-id $hostedzone_id
  ```

  Der Besitzer der übergeordneten Zone kann den Datensatz über die Route-53-Konsole oder CLI einfügen.

  - Um den DS-Eintrag mithilfe von einzufügen AWS CLI, erstellt und benennt der Besitzer der übergeordneten Zone eine JSON-Datei, die dem folgenden Beispiel ähnelt. Der Besitzer der übergeordneten Zone kann die Datei wie folgt benennen: `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"
                            }
                        ]
                    }
    ```

```
            }
        ]
    }
}
```

Führen Sie anschließend den folgenden Befehl aus:

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- Um den DS-Datensatz über die Konsole einzufügen,

  Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

  Wählen Sie im Navigationsbereich Hosted zones (Gehostete Zonen) und dann Name Ihrer gehosteten Zone und dann die Schaltfäche Create record (Datensatz erstellen) aus. Stellen Sie sicher, dass Sie Einfaches Routing für die Routing policy (Routing-Richtlinie) auswählen.

  Geben Sie im Feld Datensatzname denselben Namen wie der ein`$zone_name`, wählen Sie DS aus der Dropdownliste Datensatztyp aus, geben Sie den Wert von `$ds_record_value` in das Feld Wert ein und wählen Sie Datensätze erstellen aus.

Rollback: entfernen Sie das DS aus der übergeordneten Zone, warten Sie auf die DS-TTL und setzen Sie dann die Schritte zum Aufbau von Vertrauen zurück. Wenn die übergeordnete Zone auf Route 53 gehostet wird, kann der Besitzer der übergeordneten Zone die `Action` von `UPSERT` zu `DELETE` in der JSON-Datei ändern und die obige Beispiel-CLI erneut ausführen.

6. Warten Sie, bis die Aktualisierungen basierend auf der TTL für Ihre Domänendatensätze weitergegeben werden.

   Wenn sich die übergeordnete Zone auf dem Route 53-DNS-Dienst befindet, kann der Besitzer der übergeordneten Zone die vollständige Weitergabe über die GetChangeAPI bestätigen.

   Andernfalls können Sie die übergeordnete Zone regelmäßig auf den DS-Datensatz untersuchen und danach weitere 10 Minuten warten, um die Wahrscheinlichkeit zu erhöhen, dass die Einfügung des DS-Datensatzes vollständig propagiert wird. Beachten Sie, dass einige Registraren beispielsweise einmal täglich die DS-Einfügung geplant haben.

Wenn Sie den Delegation Signer (DS)-Datensatz in der übergeordneten Zone einführen, starten die validierten Resolver, die den DS aufgenommen haben, mit der Validierung der Antworten aus der Zone.

Um sicherzustellen, dass die Schritte zur Vertrauensbildung reibungslos verlaufen, führen Sie Folgendes aus:

1. Finden Sie das maximale NS TTL.

   Es gibt 2 Sätze von NS-Datensätzen, die Ihren Zonen zugeordnet sind:

   - Der NS-Datensatz der Delegation – dies ist der NS-Datensatz für Ihre Zone, die von der übergeordneten Zone gehalten wird. Sie können dies finden, indem Sie die folgenden Unix-Befehle ausführen (wenn Ihre Zone beispiel.com ist, ist die übergeordnete Zone com):

     ```
     dig -t NS com
     ```

     Wählen Sie einen der NS-Datensätze aus und führen Sie dann Folgendes aus:

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     Zum Beispiel:

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - Der NS-Datensatz in der Zone – dies ist der NS-Datensatz in Ihrer Zone. Sie können dies suchen, indem Sie den folgenden Unix-Befehl ausführen:

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     Zum Beispiel:

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

     Beachten Sie die maximale TTL für beide Zonen.

2. Warten Sie auf den maximalen NS TTL.

   Vor der DS-Einfügung erhalten Resolver eine signierte Antwort, validieren die Signatur jedoch nicht. Wenn der DS-Datensatz eingefügt wird, sehen Resolver ihn erst, wenn der NS-Datensatz für die Zone abläuft. Wenn Resolver den NS-Datensatz erneut abrufen, wird der DS-Datensatz dann ebenfalls zurückgegeben.

Wenn Ihr Kunde einen Resolver auf einem Host mit einer nicht synchronisierten Uhr ausführt, stellen Sie sicher, dass sich die Uhr innerhalb 1 Stunde nach der richtigen Zeit befindet.

Nach Abschluss dieses Schritts validieren alle DNSSEC-fähigen Resolver Ihre Zone.

3. Beachten Sie die Namensauflösung.

   Sie sollten beachten, dass es keine Probleme mit Resolvern gibt, die Ihre Zone validieren. Stellen Sie sicher, dass Sie auch die Zeit berücksichtigen, die Ihre Kunden benötigen, um Ihnen Probleme zu melden.

   Wir empfehlen eine Überwachung für bis zu 2 Wochen.

4. (Optional) Verlängern Sie DS und NS TTLs.

   Wenn Sie mit der Einrichtung zufrieden sind, können Sie die von Ihnen vorgenommenen TTL- und SOA-Änderungen speichern. Beachten Sie, dass Route 53 die TTL für signierte Zonen auf 1 Woche beschränkt. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

   Wenn Sie die DS TTL ändern können, empfehlen wir, dass Sie es auf 1 Stunde einstellen.

Deaktivieren der DNSSEC-Signatur

Die Schritte zum Deaktivieren der DNSSEC-Signierung in Route 53 variieren je nach Vertrauenskette, zu der Ihre gehostete Zone gehört.

Beispielsweise kann Ihre gehostete Zone eine übergeordnete Zone mit einem DS-Datensatz (Delegation Signer) als Teil einer Vertrauenskette aufweisen. Ihre gehostete Zone kann auch selbst eine übergeordnete Zone für untergeordnete Zonen sein, die die DNSSEC-Signatur aktiviert haben. Dies ist ein weiterer Teil der Vertrauenskette. Untersuchen und ermitteln Sie die vollständige Vertrauenskette für Ihre gehostete Zone, bevor Sie die DNSSEC-Signatur deaktivieren.

Die Vertrauenskette für Ihre gehostete Zone, die die DNSSEC-Signatur aktiviert, muss beim Deaktivieren der Signatur sorgfältig rückgängig gemacht werden. Um die gehostete Zone aus der Vertrauenskette zu entfernen, entfernen Sie alle DS-Datensätze, die für die Vertrauenskette vorhanden sind, die diese gehostete Zone enthält. Dies bedeutet, dass Sie Folgendes tun müssen, um:

1. Entfernen Sie alle DS-Datensätze, die diese gehostete Zone für untergeordnete Zonen enthält, die Teil einer Vertrauenskette sind.
2. Entfernen Sie den DS-Datensatz aus der übergeordneten Zone. Überspringen Sie diesen Schritt, wennn Sie über eine Vertrauensinsel verfügen (es gibt keine DS-Datensätze in der übergeordneten Zone und keine DS-Datensätze für untergeordnete Zonen in dieser Zone).
3. Wenn Sie DS-Datensätze nicht entfernen können, entfernen Sie NS-Datensätze aus der übergeordneten Zone, um die Zone aus der Vertrauenskette zu entfernen. Weitere Informationen finden Sie unter Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Mit den folgenden inkrementellen Schritten können Sie die Effektivität der einzelnen Schritte überwachen, um Probleme mit der DNS-Verfügbarkeit in Ihrer Zone zu vermeiden.

So deaktivieren Sie die DNSSEC-Signatur

1. Überwachen Sie die Verfügbarkeit der Zone.

   Sie können die Zone auf die Verfügbarkeit Ihrer Domänennamen überwachen. Dies kann Ihnen helfen, alle Probleme zu beheben, die einen Schritt zurücksetzen könnten, nachdem Sie die DNSSEC-Signatur aktiviert haben. Sie können Ihre Domänennamen mit dem größten Datenverkehr überwachen, indem Sie die Abfrageprotokollierung verwenden. Für weitere Informationen zum Einrichten einer Abfrage-Protokollierung siehe Amazon Route 53 überwachen.

   Die Überwachung kann über ein Shell-Skript oder über einen kostenpflichtigen Dienst erfolgen. Dies sollte jedoch nicht das einzige Signal sein, um festzustellen, ob ein Rollback erforderlich ist. Möglicherweise erhalten Sie auch Feedback von Ihren Kunden, da eine Domäne nicht verfügbar ist.
2. Suchen Sie die aktuelle DS TTL.

   Sie können die DS TTL finden, indem Sie den folgenden Unix-Befehl ausführen:

   ```
   dig -t DS example.com example.com
   ```
3. Suchen Sie die maximale NS TTL.

   Es gibt 2 Sätze von NS-Datensätzen, die Ihren Zonen zugeordnet sind:

- Der NS-Datensatz der Delegation – dies ist der NS-Datensatz für Ihre Zone, die von der übergeordneten Zone gehalten wird. Sie können dies suchen, indem Sie den folgenden Unix-Befehl ausführen:

  Suchen Sie zuerst den NS Ihrer übergeordneten Zone (wenn Ihre Zone beispiel.com ist, ist die übergeordnete Zone com):

  ```
  dig -t NS com
  ```

  Wählen Sie einen der NS-Datensätze aus und führen Sie dann Folgendes aus:

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  Zum Beispiel:

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- Der NS-Datensatz in der Zone – dies ist der NS-Datensatz in Ihrer Zone. Sie können dies suchen, indem Sie den folgenden Unix-Befehl ausführen:

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  Zum Beispiel:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  Beachten Sie die maximale TTL für beide Zonen.

4. Entfernen Sie den DS-Eintrag aus der übergeordneten Zone.

   Kontaktieren Sie den Besitzer der übergeordneten Zone, um den DS-Datensatz zu entfernen.

   Rollback: Fügen Sie den DS-Datensatz erneut ein, bestätigen Sie, dass die DS-Einfügung wirksam ist, und warten Sie für die maximale TTL von NS (nicht DS). Danach starten alle Resolver wieder mit der Validierung.

5. Bestätigen Sie, dass die DS-Entfernung wirksam ist.

   Wenn sich die übergeordnete Zone auf dem Route 53-DNS-Dienst befindet, kann der Besitzer der übergeordneten Zone die vollständige Weitergabe über die GetChangeAPI bestätigen.

   Andernfalls können Sie die übergeordnete Zone regelmäßig auf den DS-Datensatz untersuchen und danach weitere 10 Minuten warten, um die Wahrscheinlichkeit zu erhöhen, dass die

Entfernung des DS-Datensatzes vollständig verbreitet wird. Beachten Sie, dass einige Registraren die DS-Entfernung geplant haben, z. B. einmal am Tag.

6. Warten Sie auf die DS TTL.

   Warten Sie, bis alle Resolver den DS-Datensatz aus ihren Caches abgelaufen sind.

7. Deaktivieren Sie die DNSSEC-Signatur und deaktivieren Sie den Schlüsselsignierungsschlüssel (KSK).

   - CLI
   - Konsole

   CLI

   Rufen Sie DisableHostedZoneDNSSEC und auf. DeactivateKeySigningKey APIs

   Zum Beispiel:

```
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

   So deaktivieren Sie die DNSSEC-Signatur

   1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
   2. Wählen Sie im NavigationsbereichGehostete ZonenWählen Sie dann eine gehostete Zone aus, für die Sie die DNSSEC-Signatur deaktivieren möchten.
   3. Klicken Sie auf derDNSSECWählen Sie auf der RegisterkarteDNSSEC-Signatur deaktivierenaus.
   4. Klicken Sie auf derDNSSEC-Signatur deaktivierenWählen Sie je nach Szenario für die Zone, für die Sie die DNSSEC-Signatur deaktivieren, eine der folgenden Optionen aus.

- Nur übergeordnete Zone— Diese Zone hat eine übergeordnete Zone mit einem DS-Eintrag. In diesem Szenario müssen Sie den DS-Eintrag der übergeordneten Zone entfernen.
- Nur untergeordnete Zonen— Diese Zone verfügt über einen DS-Eintrag für eine Vertrauenskette mit einer oder mehreren untergeordneten Zonen. In diesem Szenario müssen Sie die DS-Einträge der Zone entfernen.
- Übergeordnet und untergeordnet— Diese Zone verfügt über einen DS-Datensatz für eine Vertrauenskette mit einer oder mehreren untergeordneten Zonenundeine übergeordnete Zone mit einem DS-Datensatz. Führen Sie für dieses Szenario die folgenden Schritte in aus:

  a. Entfernen Sie die DS-Einträge der Zone.

  b. Entfernen Sie den DS-Eintrag der übergeordneten Zone.

  Wenn Sie eine Insel des Vertrauens haben, können Sie diesen Schritt überspringen.

5. Bestimmen Sie die TTL für jeden DS-Datensatz, den Sie in Schritt 4 entfernen. Stellen Sie sicher, dass der längste TTL-Zeitraum abgelaufen ist.
6. Wählen Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Schritte der Reihe nach befolgt haben.
7. GebenSie disable wie gezeigt in das Feld und wählen Sie Deaktivieren aus.

So deaktivieren Sie den Schlüsselsignierungschlüssel (KSK)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Hosted Zones (Gehostete Zonen) und wählen Sie dann eine gehostete Zone aus, für die Sie den Schlüsselsignierungsschlüssel (KSK) deaktivieren möchten.
3. Wählen Sie im Abschnitt Schlüssel zur Schlüsselsignierung (KSKs) das KSK aus, das Sie deaktivieren möchten, und wählen Sie unter Aktionen die Option KSK bearbeiten aus, setzen Sie den KSK-Status auf Inaktiv und wählen Sie dann KSK speichern aus.

Rollback: Anruf und DNSSEC. ActivateKeySigningKeyEnableHostedZone APIs

Zum Beispiel:

```
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. Bestätigen Sie, dass das Deaktivieren der Zonensignierung wirksam ist.

   Vergewissern Sie sich anhand der ID aus dem `EnableHostedZoneDNSSEC()` Anruf GetChange, dass alle Route 53-DNS-Server keine Antworten mehr signieren (Status =). `INSYNC`

9. Beachten Sie die Namensauflösung.

   Sie sollten beachten, dass es keine Probleme gibt, die dazu führen, dass Resolver Ihre Zone validieren. Planen Sie 1-2 Wochen ein, um auch die Zeit zu berücksichtigen, die Ihre Kunden benötigen, um Ihnen Probleme zu melden.

10. (Optional) Bereinigen.

    Wenn Sie das Signieren nicht wieder aktivieren möchten, können Sie den KSKs durchgehenden Schlüssel bereinigen DeleteKeySigningKeyund den entsprechenden vom Kunden verwalteten Schlüssel löschen, um Kosten zu sparen.

Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC

Wenn Sie die DNSSEC-Signierung in Amazon Route 53 aktivieren, erstellt Route 53 einen Schlüssel-Signaturschlüssel (KSK). Um ein KSK zu erstellen, muss Route 53 einen vom Kunden verwalteten Schlüssel verwenden AWS Key Management Service , der DNSSEC unterstützt. In diesem Abschnitt werden die Details und Anforderungen für den vom Kunden verwalteten Schlüssel beschrieben, die bei der Arbeit mit DNSSEC hilfreich sind.

Beachten Sie Folgendes, wenn Sie mit kundenverwalteten Schlüsselverwaltete Schlüssel für DNSSEC arbeiten:

- Der kundenverwaltete Schlüssel, den Sie mit der DNSSEC-Signatur verwenden, muss sich in der Region USA Ost (Nord-Virginia) befinden.

- Der vom Kunden verwaltete Schlüssel muss ein Asymmetrische kundenverwaltete Schlüssel mit einem Schlüsselspezifikation ECC_NIST_P256 sein. Diese kundenverwalteten Schlüssel werden nur zur Signatur und Verifizierung verwendet. Hilfe bei der Erstellung eines asymmetrischen kundenverwalteten Schlüssels finden Sie unter Asymmetrische, vom Kunden verwaltete Schlüssel erstellen im Entwicklerhandbuch. AWS Key Management Service Hilfe bei der Suche nach der kryptografischen Konfiguration eines vorhandenen, vom Kunden verwalteten Schlüssels finden Sie im Entwicklerhandbuch unter Kryptografiekonfiguration von kundenverwalteten Schlüsseln anzeigen. AWS Key Management Service
- Wenn Sie einen vom Kunden verwalteten Schlüssel für die Verwendung mit DNSSEC in Route 53 selbst erstellen, müssen Sie bestimmte Schlüsselrichtlinienanweisungen einschließen, die Route 53 die erforderlichen Berechtigungen erteilen. Route 53 muss auf Ihren vom Kunden verwalteten Schlüssel zugreifen können, damit er eine KSK für Sie erstellen kann. Weitere Informationen finden Sie unter Route 53 vom Kunden verwaltete Schlüsselberechtigungen für DNSSEC-Signierung erforderlich.
- Route 53 kann einen vom Kunden verwalteten Schlüssel erstellen, den Sie ohne zusätzliche Berechtigungen AWS KMS mit der DNSSEC-Signatur verwenden können. AWS KMS Sie müssen jedoch über bestimmte Berechtigungen verfügen, wenn Sie den Schlüssel nach der Erstellung bearbeiten möchten. Die spezifischen Berechtigungen, die Sie haben müssen, sind die folgenden:`kms:UpdateKeyDescription`,`kms:UpdateAlias`, und `kms:PutKeyPolicy`.
- Beachten Sie, dass für jeden Kunden verwalteten Schlüssel, den Sie haben, separate Gebühren anfallen, unabhängig davon, ob Sie den vom Kunden verwalteten Schlüssel erstellen oder Route 53 ihn für Sie erstellt. Weitere Informationen finden Sie unter AWS Key Management Service Preise.

Arbeiten mit Schlüsseln zur Schlüsselsignierung () KSKs

Wenn Sie DNSSEC-Signaturschlüssel aktivieren, erstellt Route 53 einen Schlüssel-Signaturschlüssel (KSK). In Route 53 können Sie bis zu zwei KSKs pro gehosteter Zone haben. Nachdem Sie die DNSSEC-Signatur aktiviert haben, können Sie Ihre hinzufügen, entfernen oder bearbeiten. KSKs

Beachten Sie Folgendes, wenn Sie mit Ihrem arbeiten: KSKs

- Bevor Sie eine KSK löschen können, müssen Sie die KSK bearbeiten, um ihren Status auf Inaktiv einzustellen.

- Wenn DNSSEC-Signatur für eine gehostete Zone aktiviert ist, begrenzt Route 53 die TTL auf eine Woche. Wenn Sie eine TTL für Datensätze in der gehosteten Zone auf mehr als eine Woche festlegen, erhalten Sie keinen Fehler, aber Route 53 erzwingt eine TTL von einer Woche.
- Um einen Zonenausfall zu verhindern und Probleme mit der Nichtverfügbarkeit Ihrer Domäne zu vermeiden, müssen Sie DNSSEC-Fehler schnell beheben und beheben. Wir empfehlen Ihnen dringend, einen CloudWatch Alarm einzurichten, der Sie benachrichtigt, wenn ein `DNSSECInternalFailure` `DNSSECKeySigningKeysNeedingAction` Oder-Fehler erkannt wird. Weitere Informationen finden Sie unter Überwachung von Hosting-Zonen mit Amazon CloudWatch.
- Die in diesem Abschnitt beschriebenen KSK-Operationen ermöglichen es Ihnen, Ihre Zonen zu wechseln. KSKs Weitere Informationen und ein step-by-step Beispiel finden Sie unter DNSSEC-Schlüsselrotation im Blogbeitrag Konfiguration der DNSSEC-Signierung und -Validierung mit Amazon Route 53.

Folgen Sie den Anweisungen KSKs in den folgenden AWS-Managementkonsole Abschnitten, um damit zu arbeiten.

Hinzufügen eines Schlüsselsignaturschlüssels

Wenn Sie DNSSEC-Signatur aktivieren, erstellt Route 53 eine Schlüsselsignierung (KSK) für Sie. Sie können es auch KSKs separat hinzufügen. In Route 53 können Sie bis zu zwei KSKs pro gehosteter Zone haben.

Wenn Sie ein KSK erstellen, müssen Sie Route 53 angeben oder anfordern, um einen vom Kunden verwalteten Schlüssel zur Verwendung mit dem KSK zu erstellen. Wenn Sie einen vom Kunden verwalteten Schlüssel bereitstellen oder erstellen, gibt es mehrere Anforderungen. Weitere Informationen finden Sie unter Arbeiten mit vom Kunden verwalteten Schlüsseln für DNSSEC.

Gehen Sie folgendermaßen vor, um eine KSK in der AWS-Managementkonsole hinzuzufügen.

So fügen Sie eine KSK hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im NavigationsbereichGehostete Zonen, und wählen Sie dann eine gehostete Zone aus.

3. Wählen Sie auf der Registerkarte DNSSEC-Signierung unter Schlüssel zur Schlüsselsignierung (KSKs) die Option Zur erweiterten Ansicht wechseln und dann unter Aktionen die Option KSK hinzufügen aus.
4. UNDERKSKeinen Namen für die KSK ein, die Route 53 für Sie erstellt. Namen können nur Buchstaben, Zahlen und Unterstriche enthalten. Dieser Wert muss eindeutig sein.
5. Geben Sie den Alias für einen vom Kunden verwalteten Schlüssel ein, der für die DNSSEC-Signatur gilt, oder geben Sie einen Alias für einen neuen kundenverwalteten Schlüssel ein, den Route 53 für Sie erstellt.

   > **Note**
   >
   > Wenn Sie sich dafür entscheiden, dass Route 53 einen vom Kunden verwalteten Schlüssel erstellt, beachten Sie, dass für jeden vom Kunden verwalteten Schlüssel separate Gebühren anfallen. Weitere Informationen finden Sie unter AWS Key Management Service Preise.

6. Wählen Sie Create stack (Stack erstellen) aus.

Bearbeiten eines Schlüsselsignaturschlüssels

Sie können den Status eines KSK so bearbeiten, dassAktivoderInaktiv ist. Wenn ein KSK aktiv ist, verwendet Route 53 diese KSK für die DNSSEC-Signatur. Bevor Sie eine KSK löschen können, müssen Sie die KSK bearbeiten, um ihren Status auf Inaktiveinzustellen.

Gehen Sie folgendermaßen vor, um eine KSK im AWS-Managementkonsole zu editieren.

So bearbeiten Sie ein Tag

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im NavigationsbereichGehostete Zonen, und wählen Sie dann eine gehostete Zone aus.
3. Wählen Sie auf der Registerkarte DNSSEC-Signierung unter Schlüssel zur Schlüsselsignierung (KSKs) die Option Zur erweiterten Ansicht wechseln und dann unter Aktionen die Option KSK bearbeiten aus.
4. Nehmen Sie die gewünschten Aktualisierungen an der KSK vor und wählen SieSaveaus.

Löschen eines Schlüsselsignaturschlüssels

Bevor Sie eine KSK löschen können, müssen Sie die KSK bearbeiten, um ihren Status aufInaktiveinzustellen.

Ein Grund, warum Sie eine KSK löschen können, ist als Teil der Routine Schlüsselrotation. Es ist eine bewährte Methode, kryptografische Schlüssel regelmäßig zu drehen. Ihre Organisation verfügt möglicherweise über Standardanweisungen für das Drehen von Schlüsseln.

Befolgen Sie diese Schritte, um die AWS-Managementkonsole-Tabelle zu löschen.

So löschen Sie eine VPC

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im NavigationsbereichGehostete Zonen, und wählen Sie dann eine gehostete Zone aus.
3. Wählen Sie auf der Registerkarte DNSSEC-Signierung unter Schlüssel zur Schlüsselsignierung (KSKs) die Option Zur erweiterten Ansicht wechseln und dann unter Aktionen die Option KSK löschen aus.
4. Folgen Sie den Anweisungen, um das Löschen des KSK zu bestätigen.

KMS-Schlüssel- und ZSK-Verwaltung in Route 53

In diesem Abschnitt wird die aktuelle Vorgehensweise beschrieben, die Route 53 für Ihre Zonen mit aktivierter DNSSEC-Signatur verwendet.

> **Note**
>
> Route 53 verwendet die folgende Regel, die sich ändern könnte. Alle zukünftigen Änderungen werden die Sicherheitslage Ihrer Zone oder die von Route 53 nicht beeinträchtigen.

Wie verwendet Route 53 die mit Ihrem KSK verknüpften AWS KMS

In DNSSEC wird der KSK verwendet, um die Ressourceneintragssignatur (RRSIG) für den DNSKEY-Ressourcendatensatz zu generieren. Alle `ACTIVE` KSKs werden in der RRSIG-

Generation verwendet. Route 53 generiert eine RRSIG, indem sie die `Sign` AWS KMS API für den zugehörigen KMS-Schlüssel aufruft. Weitere Informationen finden Sie unter Signieren im AWS KMS -API-Handbuch. Diese werden RRSIGs nicht auf das in der Zone festgelegte Limit für Ressourceneinträge angerechnet.

Ein RRSIG läuft ab. Um zu verhindern, dass sie ablaufen, RRSIGs werden sie regelmäßig aktualisiert, indem sie alle ein bis sieben Tage erneuert werden. RRSIGs

Sie RRSIGs werden außerdem jedes Mal aktualisiert, wenn Sie einen der folgenden Befehle aufrufen: APIs

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Jedes Mal, wenn Route 53 eine Aktualisierung durchführt, generieren wir 15 für die nächsten Tage, falls RRSIGs auf den zugehörigen KMS-Schlüssel nicht mehr zugegriffen werden kann. Für die Schätzung der KMS-Schlüsselkosten können Sie von einer regulären Aktualisierung am Tag ausgehen. Ein KMS-Schlüssel könnte durch versehentliche Änderungen der KMS-Schlüsselrichtlinie unzugänglich werden. Der unzugängliche KMS-Schlüssel setzt den Status des zugehörigen KSK auf `ACTION_NEEDED`. Es wird dringend empfohlen, diesen Zustand zu überwachen, indem Sie bei jedem erkannten `DNSSECKeySigningKeysNeedingAction` Fehler einen CloudWatch Alarm einrichten, da bei validierenden Resolvern die Suche nach Ablauf der letzten RRSIG fehlschlägt. Weitere Informationen finden Sie unter Überwachung von Hosting-Zonen mit Amazon CloudWatch.

Wie Route 53 den ZSK Ihrer Zone verwaltet

Jede neue gehostete Zone mit aktivierter DNSSEC-Signatur hat einen `ACTIVE` Zonensignaturschlüssel (ZSK). Der ZSK wird für jede gehostete Zone separat generiert und gehört Route 53. Der aktuelle Schlüsselalgorithmus ist. ECDSAP256 SHA256

Wir werden innerhalb von sieben bis 30 Tagen nach Beginn der Signatur eine regelmäßige ZSK-Rotation in der Zone durchführen. Derzeit verwendet Route 53 die Methode „Schlüssel-Rollover vor der Veröffentlichung“. Weitere Informationen finden Sie unter Zonensignaturschlüssel-Rollover

vor der Veröffentlichung. Diese Methode führt einen anderen ZSK in die Zone ein. Die Rotation wird alle sieben bis 30 Tage wiederholt.

Route 53 unterbricht die ZSK-Rotation, wenn sich ein KSK der Zone im `ACTION_NEEDED` Status befindet, weil Route 53 nicht in der Lage sein wird, die Ressourcendatensätze RRSIGs für DNSKEY neu zu generieren, um den Änderungen im ZSK der Zone Rechnung zu tragen. Die ZSK-Rotation wird automatisch fortgesetzt, nachdem die Bedingung gelöscht wurde.

DNSSEC-Nachweise für Nichtvorhandensein in Route 53

> **Note**
>
> Route 53 verwendet die folgende Regel, die sich ändern könnte. Alle zukünftigen Änderungen werden die Sicherheitslage Ihrer Zone oder die von Route 53 nicht beeinträchtigen.

Es gibt drei Arten von Nachweisen für das Nichtvorhandensein in DNSSEC:

- Nachweis des Nichtvorhandenseins eines Datensatzes, der mit dem Abfragenamen übereinstimmt.
- Nachweis des Nichtvorhandenseins eines Typs, der mit dem Abfragetyp übereinstimmt.
- Nachweis des Vorhandenseins eines Platzhalterdatensatzes, der zur Erzeugung des Datensatzes als Antwort verwendet wird.

Route 53 implementiert den Nachweis des Nichtvorhandenseins eines Datensatzes, der mit dem Abfragenamen übereinstimmt, mithilfe der BL-Methode. Weitere Informationen finden Sie unter BL. Bei dieser Methode wird eine kompakte Darstellung des Nachweises erzeugt und das Zone Walking verhindert.

In Fällen, in denen es einen Datensatz gibt, der dem Abfragenamen, aber nicht dem Abfragetyp entspricht (z. B. bei der Abfrage nach web.example). com/AAAA but there is only web.example.com/ Apresent) geben wir einen minimalen NSEC-Datensatz (Next Secure) zurück, der alle unterstützten Ressourcendatensatztypen enthält.

Wenn Route 53 eine Antwort aus einem Platzhalterdatensatz synthetisiert, umfasst die Antwort keinen nächsten sicheren Datensatz, oder NSEC-Datensatz, für den Platzhalter. Ein solcher NSEC-Datensatz wird in einigen Implementierungen verwendet, für gewöhnlich jenen, die Offline-

Signaturen ausführen, um zu verhindern, dass die Ressourceneeintragssignaturen (RRSIG) in der Antwort wiederverwendet werden, um eine andere Antwort zu fälschen. Route 53 verwendet Online-Signierung für Datensätze, die nicht zu DNSKEY gehören, um RRSIGs spezifische Einträge für die Antwort zu generieren, die nicht für eine andere Antwort wiederverwendet werden können.

Fehlerbehebung für DNSSEC

Die Informationen in diesem Abschnitt können Ihnen helfen, Probleme mit der DNSSEC-Signatur zu lösen, einschließlich der Aktivierung und Deaktivierung sowie mit Ihren Key-Signing-Schlüsseln (). KSKs

Aktivieren der DNSSEC

Stellen Sie sicher, dass Sie die Voraussetzungen in Konfigurieren der DNSSEC-Signatur in Amazon Route 53 gelesen haben, bevor Sie mit der Aktivierung der DNSSEC-Signierung beginnen.

Deaktivieren der DNSSEC

Um DNSSEC sicher zu deaktivieren, überprüft Route 53, ob sich die Zielzone in der Vertrauenskette befindet. Es überprüft, ob das übergeordnete Element der Zielzone über NS-Datensätze der Zielzone und DS-Datensätze der Zielzone verfügt. Wenn die Zielzone nicht öffentlich auflösbar ist, z. B. wenn beim Abfragen nach NS und DS eine SERVFAIL-Antwort erhalten wird, kann Route 53 nicht feststellen, ob DNSSEC sicher deaktiviert werden kann. Sie können sich an Ihre übergeordnete Zone wenden, um diese Probleme zu beheben, und später erneut versuchen, DNSSEC zu deaktivieren.

KSK-Status lautetAktion erforderlich

Ein KSK kann seinen Status in Aktion erforderlich (oder `ACTION_NEEDED` in einen KeySigningKeyStatus) ändern, wenn Route 53 DNSSEC den Zugriff auf ein entsprechendes Objekt verliert AWS KMS key (aufgrund einer Änderung der Berechtigungen oder Löschung). AWS KMS key

Wenn der Status eines KSK Action needed (Aktion erforderlich) ist, bedeutet dies, dass es schließlich zu einem Zonenausfall für Clients kommt, die DNSSEC-validierende Resolver verwenden, und Sie müssen schnell handeln, um zu verhindern, dass eine Produktionszone nicht mehr aufgelöst werden kann.

Um das Problem zu beheben, stellen Sie sicher, dass der vom Kunden verwaltete Schlüssel, auf dem Ihre KSK basiert, aktiviert ist und über die richtigen Berechtigungen verfügt. Weitere

Informationen zu den erforderlichen Berechtigungen finden Sie unter Route 53 vom Kunden verwaltete Schlüsselberechtigungen für DNSSEC-Signierung erforderlich.

Nachdem Sie das KSK repariert haben, aktivieren Sie es erneut mithilfe der Konsole oder der AWS CLI, wie unter beschrieben. Schritt 2: Aktivieren der DNSSEC-Signatur und Erstellen einer KSK

Um dieses Problem in future zu vermeiden, sollten Sie erwägen, eine Amazon CloudWatch Metrik hinzuzufügen, um den Status des KSK nachzuverfolgen, wie unter vorgeschlagen. Konfigurieren der DNSSEC-Signatur in Amazon Route 53

KSK-Status lautetInternal failure (Interner Fehler)

Wenn ein KSK den Status Interner Fehler (oder `INTERNAL_FAILURE` einen KeySigningKeyStatus) hat, können Sie nicht mit anderen DNSSEC-Entitäten arbeiten, bis das Problem behoben ist. Sie müssen Maßnahmen ergreifen, bevor Sie mit der DNSSEC-Signatur arbeiten können, einschließlich der Arbeit mit dieser KSK oder Ihrer anderen KSK.

Um das Problem zu beheben, versuchen Sie erneut, KSK zu aktivieren oder zu deaktivieren.

Um das Problem bei der Arbeit mit dem zu beheben APIs, versuchen Sie, das Signieren zu aktivieren (EnableHostedZoneDNSSEC) oder das Signieren zu deaktivieren (DNSSEC). DisableHostedZone

Es ist wichtig, dass SieInternal failure (Interner Fehler)umgehend Probleme. Sie können keine weiteren Änderungen an der gehosteten Zone vornehmen, bis Sie das Problem behoben haben, mit Ausnahme der Vorgänge zum Beheben des Internal failure (Interner Fehler).

Wird AWS Cloud Map zum Erstellen von Datensätzen und Zustandsprüfungen verwendet

Wenn Sie Internetdatenverkehr oder Datenverkehr innerhalb einer Amazon VPC an Anwendungskomponenten oder Microservices weiterleiten möchten, können Sie AWS Cloud Map zum automatischen Erstellen von Datensätzen und optional zum Erstellen von Zustandsprüfungen verwenden. Weitere Informationen finden Sie im AWS Cloud Map -Entwicklerhandbuch.

DNS-Einschränkungen und Verhaltensweisen

DNS-Messaging unterliegt Faktoren, die die Erstellung und Verwendung gehosteter Zonen und Datensätze beeinflussen. In diesem Abschnitt werden diese Faktoren erläutert.

Maximale Antwortgröße

Um die DNS-Standards einzuhalten, haben über UDP gesendete Antworten eine Größe von höchstens 512 Byte. Antworten mit mehr als 512 Byte werden abgeschnitten, und der Auflösungsdienst muss die Anforderung erneut über TCP senden. Wenn der Auflösungsdienst EDNS0 unterstützt (gemäß RFC 2671) und die EDNS0-Option zu Amazon Route 53 anbietet, genehmigt Route 53 Antworten mit bis zu 4096 Byte über UDP, ohne Kürzung.

Autoritative Abschnittsverarbeitung

Für erfolgreiche Abfragen hängt Route 53 Namensserver-Datensätze (NS) für die entsprechende gehostete Zone an den Authority-Abschnitt der DNS-Antwort an. Bei Namen, die nicht gefunden werden (NXDOMAIN-Antworten), hängt Route 53 den SOA-Datensatz (Start of Authority, Autoritätsursprung) (gemäß RFC 1035) für die entsprechende gehostete Zone an den Authority-Abschnitt der DNS-Antwort an.

Zusätzliche Abschnittsverarbeitung

Route 53 hängt Datensätze an den Additional-Abschnitt an. Wenn die Datensätze bekannt und geeignet sind, fügt der Service A- oder AAAA-Datensätze für jedes Ziel eines MX-, CNAME-, NS- oder SRV-Datensatzes in den Answer-Abschnitt ein. Weitere Informationen zu diesen DNS-Datensatztypen finden Sie unter Unterstützte DNS-Datensatztypen.

Verwandte Themen

Informationen zur Übertragung der Domainregistrierung (nicht nur DNS-Hosting) auf Route 53 finden Sie in den folgenden Themen:

- Checkliste vor der Übertragung für Domainübertragungen— Füllen Sie diese Checkliste aus, bevor Sie die Domainregistrierung übertragen, um häufige Übertragungsfehler zu vermeiden.
- Übertragen der Registrierung für eine Domain an Amazon Route 53— Step-by-step Verfahren zur Übertragung der Domainregistrierung von einem anderen Registrar auf Route 53.

- Übertragen von Domänen— Überblick über alle Optionen für die Domainübertragung, einschließlich Übertragungen zwischen AWS Konten.

Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr

Traffic Flow vereinfacht den Prozess der Erstellung und Verwaltung von Aufzeichnungen in großen und komplexen Konfigurationen erheblich.

Das Verwalten von verknüpften Datensätzen in einer gehosteten Zone kann unter folgenden Umständen eine Herausforderung darstellen:

- Sie verfügen über viele Ressourcen, die denselben Vorgang ausführen, z. B. Webserver, die Datenverkehr für dieselbe Domäne bereitstellen.
- Sie möchten eine komplexe Struktur von Datensätzen mithilfe von Aliasdatensätzen und einer Kombination von Route-53-Routing-Richtlinien, wie Latenz, Failover und gewichtet, erstellen.

Vorteile von Traffic Flow

Um die Nachverfolgung der Datensätze und ihrer Beziehungen zu erleichtern, vereinfacht Traffic Flow die Erstellung von DNS-Einträgen mit den folgenden Funktionen:

Visual editor (Visueller Editor)

Mit dem visuellen Editor von Traffic Flow können Sie komplexe Datensatzbäume erstellen und die Beziehungen zwischen den Datensätzen anzeigen. Beispielsweise können Sie eine Konfiguration erstellen, in der Latenzaliasdatensätze gewichtete Datensätze referenzieren und die gewichteten Datensätze auf Ihre Ressourcen in mehreren AWS-Regionen verweisen. Jede Konfiguration wird als Datenverkehrsrichtlinie bezeichnet. Sie können beliebig viele Datenverkehrsrichtlinien kostenlos erstellen.

Versionsverwaltung

Sie können mehrere Versionen einer Datenverkehrsrichtlinie erstellen, damit Sie bei einer Änderung der Konfiguration nicht von vorn beginnen müssen. Alte Versionen bestehen weiterhin, bis Sie sie löschen. Es gibt ein Standardlimit von 1000 Versionen pro Datenverkehrsrichtlinie. Sie können jeder Version optional eine Beschreibung geben.

Automatische Datensatzerstellung und -aktualisierung

Eine Datenverkehrsrichtlinie kann Dutzende oder sogar Hunderte von Datensätzen darstellen. Mit Traffic Flow können Sie all diese Datensätze automatisch erstellen, indem Sie einen Datensatz

zur Verkehrspolitik erstellen. Sie geben die gehostete Zone und den Namen des Datensatzes im Stammverzeichnis der Struktur an, z. B. example.com oder www.example.com. Route 53 erstellt daraufhin automatisch alle anderen Datensätze in der Struktur. Der Stammdatensatz, der Datenverkehrsrichtliniendatensatz, wird in der Liste der Datensätze für Ihre gehostete Zone angezeigt. Alle anderen Datensätze werden ausgeblendet.

Wenn Sie eine neue Version einer Datenverkehrsrichtlinie erstellen, können Sie die mit der vorherigen Version der Datenverkehrsrichtlinie erstellten Datensätze für Datenverkehrsrichtlinien selektiv aktualisieren. Wenn Sie einen Datensatz für eine Datenverkehrsrichtlinie aktualisieren, aktualisiert Route 53 automatisch alle anderen Datensätze in der Struktur. Sie können Änderungen auch schnell zurücksetzen, indem Sie einen Datensatz für die Datenverkehrsrichtlinie erneut aktualisieren, um eine vorherige Version einer Datenverkehrsrichtlinie zu verwenden.

> **Note**
>
> Sie können Traffic Flow verwenden, um Datensätze nur in öffentlich gehosteten Zonen zu erstellen.

Routing-Richtlinie auf Grundlage der geografischen Nähe

Wenn Sie Traffic Flow verwenden, können Sie mithilfe der Geoproximitätskarte im Visual Editor von Traffic Flow intuitiver nachvollziehen, wie der Verkehr zu den einzelnen globalen Endpunkten geleitet wird. Weitere Informationen finden Sie unter Geoproximity-Routing.

Wiederverwendung für mehrere Datensätze in verschiedenen gehosteten Zonen

Sie können eine Datenverkehrsrichtlinie verwenden, um Datensätze automatisch in mehreren öffentlichen gehosteten Zonen zu erstellen. Wenn Sie beispielsweise dieselben Webserver für mehrere Domänennamen verwenden, können Sie dieselbe Datenverkehrsrichtlinie nutzen, um Datensätze für Datenverkehrsrichtlinien in den gehosteten Zonen für example.com, example.org und example.net zu erstellen.

Wenn ein Client eine Abfrage für den Namen des Stammdatensatzes übermittelt, z. B. example.com oder www.example.com, antwortet Route 53 auf die Abfrage basierend auf der Konfiguration in der Datenverkehrsrichtlinie, die Sie zum Erstellen des entsprechenden Datensatzes für die Datenverkehrsrichtlinie verwendet haben.

Es gibt eine monatliche Gebühr für jeden Datensatz der Datenverkehrsrichtlinie. Weitere Informationen finden Sie im Abschnitt „Datenverkehrsfluss“ von Amazon Route 53 – Preise.

Um diese Kosten zu minimieren, können Sie einen oder mehrere Aliasdatensätze in einer gehosteten Zone erstellen, die auf einen Datensatz für die Datenverkehrsrichtlinie in dieser gehosteten Zone verweisen. Beispielsweise können Sie einen Datensatz für Datenverkehrsrichtlinien für example.com und dann einen Aliasdatensatz für www.example.com erstellen, der auf den Datensatz für die Datenverkehrsrichtlinie verweist.

Erstellen und Verwalten von Datenverkehrsrichtlinien

Themen

Erstellen einer Datenverkehrsrichtlinie

Um eine Datenverkehrsrichtlinie zu erstellen, führen Sie die folgenden Schritte aus.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So erstellen Sie eine Datenverkehrsrichtlinie

1. Entwerfen Sie Ihre Konfiguration. Informationen darüber, wie komplexe DNS-Routing-Konfigurationen funktionieren, finden Sie unter Konfigurieren von DNS Failover in Amazon Route 53-Zustandsprüfungen erstellen .
2. Basierend auf dem Entwurf für Ihre Konfiguration erstellen Sie die Zustandsprüfungen, die Sie für Ihre Endpunkte verwenden möchten.
3. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
4. Wählen Sie im Navigationsbereich Traffic policies aus.
5. Klicken Sie auf Create traffic policy.
6. Geben Sie einen Namen und eine optionale Beschreibung ein, und wählen Sie dann Weiter.
7. Wählen Sie im Editor im Eigenschaftenbereich den Typ des DNS-Ressourceneintrags aus. Dieser Typ wird allen Ressourceneinträgen zugewiesen, die Sie für diese Verkehrsrichtlinie erstellen.

   Wählen Sie Bestätigen aus. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.
8. Wählen Sie auf der Editor-Seite Connect und wählen Sie dann eine der Optionen Neue Routing-Regel, Neuer Endpunkt, Bestehende Routing-Regel oder Existierender Endpunkt aus. Wenn Sie eine Neue Routing-Regel ausgewählt haben, wählen Sie im Eigenschaftenbereich die Routing-Regel aus und klicken Sie auf Bestätigen. Geben Sie dann im Eigenschaftenbereich die entsprechenden Werte ein. Wiederholen Sie diesen Vorgang, bis Ihre Richtlinie abgeschlossen ist. Weitere Informationen zu den Werten für die einzelnen Verbindungstypen finden Sie unterAngegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

   Sie können Regeln, Endpunkte und Verzweigungen einer Datenverkehrsrichtlinie auf folgende Weise löschen:

   - Um eine Regel oder einen Endpunkt zu löschen, wählen Sie die Regel oder den Endpunkt im Editor aus und klicken Sie dann im Eigenschaftenbereich auf Löschen.

> **Important**
>
> Wenn Sie eine Regel löschen, die untergeordnete Regeln und Endpunkte hat, löscht Amazon Route 53 auch alle untergeordneten Elemente.

- Wenn Sie zwei Regeln mit derselben untergeordneten Regel oder demselben untergeordneten Endpunkt verbinden und eine der Verbindungen löschen möchten, wählen Sie die Verbindung aus, die Sie löschen möchten, und wählen Sie im Eigenschaftenbereich für diese Verbindung die Option Löschen aus.

9. Wählen Sie Richtlinie erstellen aus.
10. Verwenden Sie auf der Seite „Richtlinieneinträge erstellen“ die neue Verkehrsrichtlinie, um einen oder mehrere Richtlinieneinträge in einer gehosteten Zone zu erstellen. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben. Darüber hinaus können Sie Richtliniendatensätze zu einem späteren Zeitpunkt erstellen, entweder in derselben gehosteten -Zone oder in zusätzlichen gehosteten Zonen.

    Wenn Sie jetzt keine Richtlinieneinträge erstellen möchten, wählen Sie Abbrechen. In der Konsole wird die Liste der Verkehrsrichtlinien und Richtliniendatensätze angezeigt, die Sie mit dem aktuellen AWS Konto erstellt haben.
11. Wenn Sie im vorherigen Schritt Einstellungen für Richtlinieneinträge angegeben haben, wählen Sie Richtlinieneinträge erstellen aus.

Old console

So erstellen Sie eine Datenverkehrsrichtlinie

1. Entwerfen Sie Ihre Konfiguration. Informationen darüber, wie komplexe DNS-Routing-Konfigurationen funktionieren, finden Sie unter Konfigurieren von DNS Failover in Amazon Route 53-Zustandsprüfungen erstellen .
2. Basierend auf dem Entwurf für Ihre Konfiguration erstellen Sie die Zustandsprüfungen, die Sie für Ihre Endpunkte verwenden möchten.
3. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
4. Wählen Sie im Navigationsbereich Traffic policies aus.

5. Klicken Sie auf Create traffic policy.
6. Geben Sie auf der Seite Name policy die entsprechenden Werte an. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Create traffic policy (Datenverkehrsrichtlinie erstellen) Name der Richtlinie v1 die entsprechenden Werte ein. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

   Sie können Regeln, Endpunkte und Verzweigungen einer Datenverkehrsrichtlinie auf folgende Weise löschen:

   - Um eine Regel oder einen Endpunkt zu löschen, klicken Sie auf das x in der rechten oberen Ecke der Konsole

     > **Important**
     >
     > Wenn Sie eine Regel löschen, die untergeordnete Regeln und Endpunkte hat, löscht Amazon Route 53 auch alle untergeordneten Elemente.

   - Wenn Sie zwei Regeln mit derselben untergeordneten Regel oder einem Endpunkt verbinden und eine der Verbindungen löschen möchten, zeigen Sie mit dem Mauszeiger auf die Verbindung, die Sie löschen möchten, und klicken Sie auf das x für diese Verbindung.
9. Klicken Sie auf Create traffic policy.
10. Optional: Verwenden Sie auf der Seite Create policy records with traffic policy (Richtliniendatensätze mit Datenverkehrsrichtlinie erstellen) die neue Datenverkehrsrichtlinie, um einen oder mehrere Richtliniendatensätze in einer gehosteten Zone zu erstellen. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben. Darüber hinaus können Sie Richtliniendatensätze zu einem späteren Zeitpunkt erstellen, entweder in derselben gehosteten -Zone oder in zusätzlichen gehosteten Zonen.

    Wenn Sie jetzt keine Richtlinieneinträge erstellen möchten, wählen Sie „Diesen Schritt überspringen“. In der Konsole wird dann die Liste der Verkehrsrichtlinien und Richtliniendatensätze angezeigt, die Sie mit dem aktuellen AWS Konto erstellt haben.
11. Wenn Sie im vorhergehenden Schritt angegebenen Einstellungen für Richtliniendatensätze angegeben haben, wählen Sie Create policy record.

Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden. Die folgende Liste gilt für beide Konsolen, sofern nicht anders angegeben.

Beim Erstellen einer Datenverkehrsrichtlinie geben Sie die folgenden Werte an.

-
-
-
-
-
-
-
-

Richtlinienname

Geben Sie einen Namen zur Beschreibung der Datenverkehrsrichtlinie ein. Dieser Wert wird in der Liste der Datenverkehrsrichtlinien in der Konsole angezeigt. Sie können den Namen einer Datenverkehrsrichtlinie nicht mehr ändern, nachdem Sie sie erstellt haben.

Version

Dieser Wert wird automatisch von Amazon Route 53 zugewiesen, wenn Sie eine Datenverkehrsrichtlinie oder eine neue Version einer vorhandenen Richtlinie erstellen.

Versionsbeschreibung

Geben Sie eine Beschreibung für diese Version der Datenverkehrsrichtlinie ein. Dieser Wert wird in der Liste der Versionen der Datenverkehrsrichtlinien in der Konsole angezeigt.

DNS-Typ

Wählen Sie den DNS-Typ aus, den Amazon Route 53 allen Datensätzen zuweisen soll, wenn Sie eine Richtlinie mithilfe dieser Datenverkehrsrichtlinie erstellen. Eine Liste der unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

> **Important**
>
> Wenn Sie eine neue Version einer vorhandenen Datenverkehrsrichtlinie erstellen, können Sie den DNS-Typ ändern. Es ist jedoch nicht möglich, einen Richtliniendatensatz zu bearbeiten und eine Version der Datenverkehrsrichtlinie auszuwählen, deren DNS-Typ sich von der Version der Datenverkehrsrichtlinie unterscheidet, mit der Sie die Datenverkehrsrichtlinie erstellt haben. Wenn Sie beispielsweise einen Richtliniendatensatz unter Verwendung einer Version der Datenverkehrsrichtlinie erstellt haben, die den DNS-Typ A hat, können Sie den Richtliniendatensatz nicht ändern und eine Datenverkehrsrichtlinien-Version auswählen, die einen anderen Wert für DNS-Typ hat.

Wenn Sie den Datenverkehr an die folgenden AWS Ressourcen weiterleiten möchten, wählen Sie den entsprechenden Wert:

- CloudFront Verteilung — Wählen Sie A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im IPv6 Format.

  > **Note**
  >
  > CloudFront Alias-Endpunkte unterstützen den Evaluate Health Check nicht. Sie können jedoch eine Integritätsprüfung erstellen, um CloudFront Endgeräte zu überwachen. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

- ELB Application Load Balancer — Wählen Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im Format. IPv6
- ELB Classic Load Balancer — Wählen Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im Format. IPv6
- ELB Network Load Balancer — Wählen Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im Format. IPv6
- Elastic Beanstalk Beanstalk-Umgebung: Wählen Sie A: IP-Adresse im IPv4 Format.

- Als Website-Endpunkt konfigurierter Amazon S3 S3-Bucket: Wählen Sie im IPv4 Format A: IP-Adresse.

Connect to (Verbinden mit)

Wählen Sie die entsprechende Regel oder den Endpunkt basierend auf dem Entwurf für Ihre Konfiguration aus.

Failover-Regel

Verwenden Sie diese Option, wenn Sie Aktiv/Passiv-Failover konfigurieren möchten, bei dem eine Ressource den gesamten Datenverkehr übernimmt, wenn sie verfügbar ist, und die andere Ressource den gesamten Datenverkehr übernimmt, wenn die erste Ressource nicht verfügbar ist.

Weitere Informationen finden Sie unter Aktiv/Passiv-Failover.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Geolocation-Regel

Wählen Sie diese Option, wenn Sie möchten, dass Amazon Route 53 DNS-Abfragen basierend auf dem Standort Ihrer Benutzer beantwortet.

Weitere Informationen finden Sie unter Geolocation-Routing.

Wenn Sie Geolocation rule wählen, wählen Sie auch das Land oder den Bundesstaat in den USA aus, aus dem die Anfragen gesendet werden.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz

weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Latenz-Regel

Wählen Sie diese Option, wenn Sie über Ressourcen in mehreren EC2 Amazon-Rechenzentren verfügen, die dieselbe Funktion ausführen, und Sie möchten, dass Route 53 auf DNS-Abfragen mit den Ressourcen reagiert, die die beste Latenz bieten.

Wenn Sie Latenzregel wählen, wählen Sie auch eine AWS-Region aus.

Weitere Informationen finden Sie unter Latenzbasiertes Routing.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Geoproximity rule

Wählen Sie diese Option aus, wenn Route 53 auf DNS-Abfragen basierend auf dem Standort Ihrer Ressourcen und optional basierend auf einem von Ihnen angegebenen Bias-Wert antworten soll. Der Bias-Wert ermöglicht Ihnen, mehr Datenverkehr zu einer Ressource zu senden oder weniger Datenverkehr von einer Ressource zu senden.

Wenn Sie Geoproximity rule wählen, geben Sie die folgenden Werte ein:

Endpunktstandort

Wählen Sie einen geeignete Wert aus:

- Benutzerdefiniert (Koordinaten eingeben) — Wenn Ihr Endpunkt keine AWS Ressource ist, wählen Sie Benutzerdefiniert (Koordinaten eingeben).

- A AWS-Region — Wenn es sich bei Ihrem Endpunkt um eine AWS Ressource handelt, wählen Sie AWS-Region die aus, in der Sie die Ressource erstellt haben.
- Eine AWS lokale Zone — Wenn es sich bei Ihrem Endpunkt um eine AWS Ressource handelt, wählen Sie die AWS Lokale Zone aus, in der Sie die Ressource erstellt haben.

Wenn Sie AWS Local Zones verwenden, müssen Sie sie zuerst aktivieren. Weitere Informationen finden Sie im Benutzerhandbuch zu AWS Local Zones unter Erste Schritte mit Local Zones.

Informationen zu verfügbaren Local Zones finden Sie unter Local Zones von AWS – Standorte.

Weitere Informationen zum Unterschied zwischen AWS-Regionen und Local Zones finden Sie unter Regionen und Zonen im EC2 Amazon-Benutzerhandbuch.

> **Important**
>
> Eine einzelne Routing-Richtlinie auf Grundlage der geografischen Nähe kann nicht zwei oder mehr Standorte enthalten, die sich geografisch innerhalb derselben Metropolregion befinden.
> Darüber hinaus liegen einige AWS-Regionen und Local Zones, wie US West (Oregon) und Portland, USA, zu nahe beieinander, um im Rahmen derselben Geoproximity-Routing-Richtlinie verwendet zu werden. Wenn Sie den Verkehr zu mehr als einem Standort innerhalb derselben Metropolregion weiterleiten möchten, definieren Sie stattdessen eine Routing-Richtlinie basierend auf der geografischen Nähe, die zu einer 50/50-Regel für gewichtetes Routing (WRR) für zwei verschiedene Endpunkte in der Region führt, wodurch der Verkehr gleichmäßig auf diese Endpunkte verteilt wird.

Koordinaten

Wenn Sie Custom (enter coordinates) für Endpoint location wählen, geben Sie den Breiten- und Längengrad des Standorts der Ressource ein. Beachten Sie Folgendes:

- Der Breitengrad gibt an, ob der Standort südlich (negativ) oder nördlich (positiv) des Äquators liegt. Gültige Werte sind -90 Grad bis 90 Grad.
- Der Längengrad gibt an, ob der Standort westlich (negativ) oder östlich (positiv) des Nullmeridians liegt. Gültige Werte sind -180 Grad bis 180 Grad.

- Sie können Breiten- und Längengrad in einigen Online-Mapping-Anwendungen erhalten. Beispielsweise gibt in Google Maps die URL für einen Standort den Breiten- und Längengrad an:

  https://www.google.com/maps/@ 47.6086111, - 122.3409953 ,20z

- Sie können aus Präzisionsgründen bis zu zwei Dezimalstellen eingeben, z. B. 47.63. Wenn Sie einen Wert mit größerer Präzision angeben, schneidet Route 53 den Wert auf zwei Stellen nach dem Dezimalzeichen ab. In Bezug auf den Breiten- und Längengrad am Äquator entsprechen 0,01 Grad ungefähr 1,1 Kilometer.

Bias

Um optional die Größe der geografischen Region zu ändern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie für Bias den entsprechenden Wert an:

- Um die Größe der geografischen Region zu erweitern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie für den Bias-Wert eine positive Ganzzahl von 1 bis 99 an. Route 53 verkleinert die Größe der angrenzenden Regionen.
- Um die Größe der geografischen Region zu verkleinern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie einen negativen Bias-Wert zwischen -1 und -99 an. Route 53 erweitert die Größe der angrenzenden Regionen.

> **Important**
>
> Die Auswirkungen bei einer Änderungen des Wertes von Bias sind relativ, d. h. abhängig vom Standort anderer Ressourcen, und nicht absolut, d. h. auf der Entfernung basierend. Daher können die Auswirkungen einer Änderung nur schwer vorhergesagt werden. Abhängig vom Standort Ihrer Ressourcen kann eine Änderung des Bias-Werts zwischen 10 und 15 beispielsweise den Unterschied zwischen der Hinzufügung oder dem Abzug einer erheblichen Menge an Datenverkehr zum oder aus dem Bereich von New York City bedeuten. Es wird empfohlen, den Bias-Wert in kleinen Schritte zu ändern, die Ergebnisse auszuwerten und anschließend weitere Änderungen vorzunehmen, wenn angemessen.

Weitere Informationen finden Sie unter Geoproximity-Routing.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Mehrwertige Antwort-Regel

Wählen Sie diese Option aus, wenn Sie möchten, dass Route 53 auf DNS-Abfragen mit bis zu acht fehlerfreien Antworten reagiert, die zufällig ausgewählt wurden.

Weitere Informationen finden Sie unter Mehrwertiges Antwort-Routing.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Gewichtungs-Regel

Wählen Sie diese Option aus, wenn Sie über mehrere Ressourcen verfügen, die die gleiche Funktion erfüllen (z. B. Webserver für die gleiche Website), und möchten, dass Route 53 Datenverkehr in den von Ihnen vorgegebenen Proportionen an diese Ressourcen weiterleitet (z. B. ein Drittel an einen Server und zwei Drittel an den anderen).

Wenn Sie Weighted rule (Gewichtete Regel) wählen, geben Sie die Gewichtung ein, die Sie auf diese Regel anwenden möchten.

Weitere Informationen finden Sie unter Gewichtetes Routing.

> **Note**
>
> Die Option „Zustand des Ziels bewerten“ ist standardmäßig aktiviert und bewertet den Zustand des Zielendpunkts, zu dem der Datenverkehr über einen Aliasdatensatz weitergeleitet wird. Wenn Ihr Endpunkt keinen DNS-Datenverkehr über einen Aliasdatensatz empfängt, deaktivieren Sie diesen und führen Sie eine Zustandsprüfung durch, wenn Sie den Zustand des Endpunkts überwachen möchten. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Endpoint

Wählen Sie diese Option, um die Ressource anzugeben, an die Sie DNS-Abfragen weiterleiten möchten, z. B. eine CloudFront Distribution oder einen Elastic Load Balancing Load Balancer.

Vorhandene Regel

Wählen Sie diese Option, wenn Sie DNS-Abfragen zu einer vorhandenen Regel in dieser Datenverkehrsrichtlinie leiten möchten. Sie können beispielsweise zwei oder mehr Geolocation-Regeln erstellen, die Abfragen für verschiedene Länder an dieselbe Failover-Regel leiten. Die Failover-Regel kann dann Abfragen an zwei Elastic Load Balancing Load Balancer weiterleiten.

Diese Option ist nicht verfügbar, wenn die Datenverkehrsrichtlinie keine Regeln enthält.

Vorhandener Endpunkt

Wählen Sie diese Option, wenn Sie DNS-Abfragen zu einem vorhandenen Endpunkt leiten möchten. Wenn Sie beispielsweise über zwei Failover-Regeln verfügen, können Sie ggf. DNS-Abfragen für beide Optionen vom Typ Bei Failover (sekundär) an den gleichen Elastic Load Balancing Load Balancer weiterleiten.

Diese Option ist nicht verfügbar, wenn die Datenverkehrsrichtlinie keine Endpunkte enthält.

Werttyp

Wählen Sie eine geeignete Option aus:

CloudFront Verteilung

Wählen Sie diese Option, wenn Sie den Verkehr an eine CloudFront Verteilung weiterleiten möchten. Die Option ist nur verfügbar, wenn Sie A: IP-Adresse im IPv4 Format für DNS-Typ oder AAAA: IP-Adresse im IPv6 Format für DNS-Typ ausgewählt haben.

> **Note**
>
> CloudFront Alias-Endpunkte unterstützen den Evaluate Health Check nicht. Sie können jedoch eine Integritätsprüfung erstellen, um CloudFront Endgeräte zu überwachen. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

ELB Application Load Balancer

Wählen Sie diese Option aus, wenn Sie Datenverkehr an einen Elastic Load Balancing Application Load Balancer weiterleiten möchten. Die Option ist nur verfügbar, wenn Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im IPv6 Format für DNS-Typ ausgewählt haben.

ELB Classic Load Balancer

Wählen Sie diese Option aus, wenn Sie Datenverkehr an einen Elastic Load Balancing Classic Load Balancer weiterleiten möchten. Die Option ist nur verfügbar, wenn Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im IPv6 Format für DNS-Typ ausgewählt haben.

ELB Network Load Balancer

Wählen Sie diese Option aus, wenn Sie Datenverkehr an einen Elastic Load Balancing Network Load Balancer weiterleiten möchten. Die Option ist nur verfügbar, wenn Sie entweder A: IP-Adresse im IPv4 Format oder AAAA: IP-Adresse im IPv6 Format für DNS-Typ ausgewählt haben.

Elastic Beanstalk-Umgebung

Wählen Sie diese Option aus, wenn Sie Datenverkehr an eine Elastic-Beanstalk-Umgebung weiterleiten möchten. Die Option ist nur verfügbar, wenn Sie A: IP-Adresse im IPv4 Format für den DNS-Typ ausgewählt haben.

S3-Website-Endpunkt

Wählen Sie diese Option, wenn Sie Datenverkehr an einen Amazon-S3-Bucket leiten möchten, der als Website-Endpunkt konfiguriert ist. Die Option ist nur verfügbar, wenn Sie A: IP-Adresse im IPv4 Format für den DNS-Typ ausgewählt haben.

Werteingabe für DNS type

Wählen Sie diese Option, wenn Sie möchten, dass Route 53 auf DNS-Abfragen mit den Wert im Feld Wert antwortet. Wenn Sie beispielsweise den Wert A für DNS type ausgewählt haben, als Sie diese Datenverkehrsrichtlinie erstellt haben, wird diese Option in der Liste Value type als Type A value angezeigt. Dazu müssen Sie eine IP-Adresse im IPv4 Format „Wert“ eingeben. Route 53 antwortet auf DNS-Abfragen, die an diesen Endpunkt geleitet werden, mit der IP-Adresse im Feld Wert.

Wert

Wählen Sie einen Wert aus oder geben Sie einen Wert basierend auf der gewählten Option für Value type (Werttyp) ein:

CloudFront Verteilung

Wählen Sie eine CloudFront Verteilung aus der Liste der Verteilungen aus, die dem AWS Girokonto zugeordnet sind.

ELB Application Load Balancer

Wählen Sie einen Elastic Load Balancing Application Load Balancer aus der Liste der Load Balancer aus, die dem aktuellen AWS Konto zugeordnet sind.

ELB Classic Load Balancer

Wählen Sie einen Elastic Load Balancing Classic-Load Balancer aus der Liste der Load Balancer aus, die dem AWS Girokonto zugeordnet sind.

ELB Network Load Balancer

Wählen Sie einen Elastic Load Balancing Network Load Balancer aus der Liste der Load Balancer aus, die dem aktuellen AWS Konto zugeordnet sind.

Elastic Beanstalk-Umgebung

Wählen Sie eine Elastic-Beanstalk-Umgebung aus der Liste der Umgebungen aus, die dem aktuellen AWS-Konto zugeordnet sind.

S3-Website-Endpunkt

Wählen Sie einen Amazon S3 S3-Bucket aus der Liste der Amazon S3 S3-Buckets aus, die als Website-Endpunkte konfiguriert sind und mit dem aktuellen AWS Konto verknüpft sind.

> **Important**
>
> Wenn Sie einen Richtliniendatensatz basierend auf dieser Datenverkehrsrichtlinie erstellen, muss der hier ausgewählte Bucket mit dem Domänennamen (z. B. www.example.com) übereinstimmen, den Sie für Policy record DNS name im Richtliniendatensatz angeben. Wenn Wert und Richtliniendatensatz-DNS-Name nicht übereinstimmen, antwortet Amazon S3 nicht auf DNS-Abfragen für den Domänennamen.

Werteingabe für DNS type

Geben Sie einen Wert ein, der dem Wert entspricht, den Sie für DNS type zu Beginn dieser Datenverkehrsrichtlinie eingegeben haben. Wenn Sie beispielsweise MX für DNS type (DNS-Typ) ausgewählt haben, geben Sie zwei Werte ein: die Priorität, die Sie einem E-Mail-Server zuweisen möchten, und den Domänennamen des E-Mail-Servers (beispielsweise `10 sydney.mail.example.com`).

Weitere Informationen zu unterstützten DNS-Typen finden Sie unter Unterstützte DNS-Datensatztypen.

Schlüssel (nur neue Konsole)

Geben Sie einen benutzerfreundlichen Namen für eine Routing-Regel oder einen Endpunkt für Key ein. Dieser Wert wird als Name eines Knotens im Editor angezeigt.

Anzeigen einer Karte, die die Auswirkungen der Einstellungen für geografische Nähe darstellt

Mit einer Geoproximitätsregel können Sie die Standorte Ihrer Ressourcen angeben, sowohl in AWS-Regionen Local Zones als auch, unter Verwendung von Breitengrad und Längengrad, an anderen AWS Orten. Wenn Sie eine Regel für geografische Nähe erstellen, leitet Route 53 Internetdatenverkehr standardmäßig an die Ressource weiter, die Ihren Benutzern am nächsten ist. Sie können auch mehr oder weniger Datenverkehr an eine Ressource weiterleiten, indem Sie einen Bias-Wert angeben, der den geografischen Bereich vergrößert oder verkleinert, aus dem Datenverkehr an eine Ressource weitergeleitet wird. Weitere Informationen über Weiterleitung aufgrund der geografischen Nähe finden Sie unter Geoproximity-Routing.

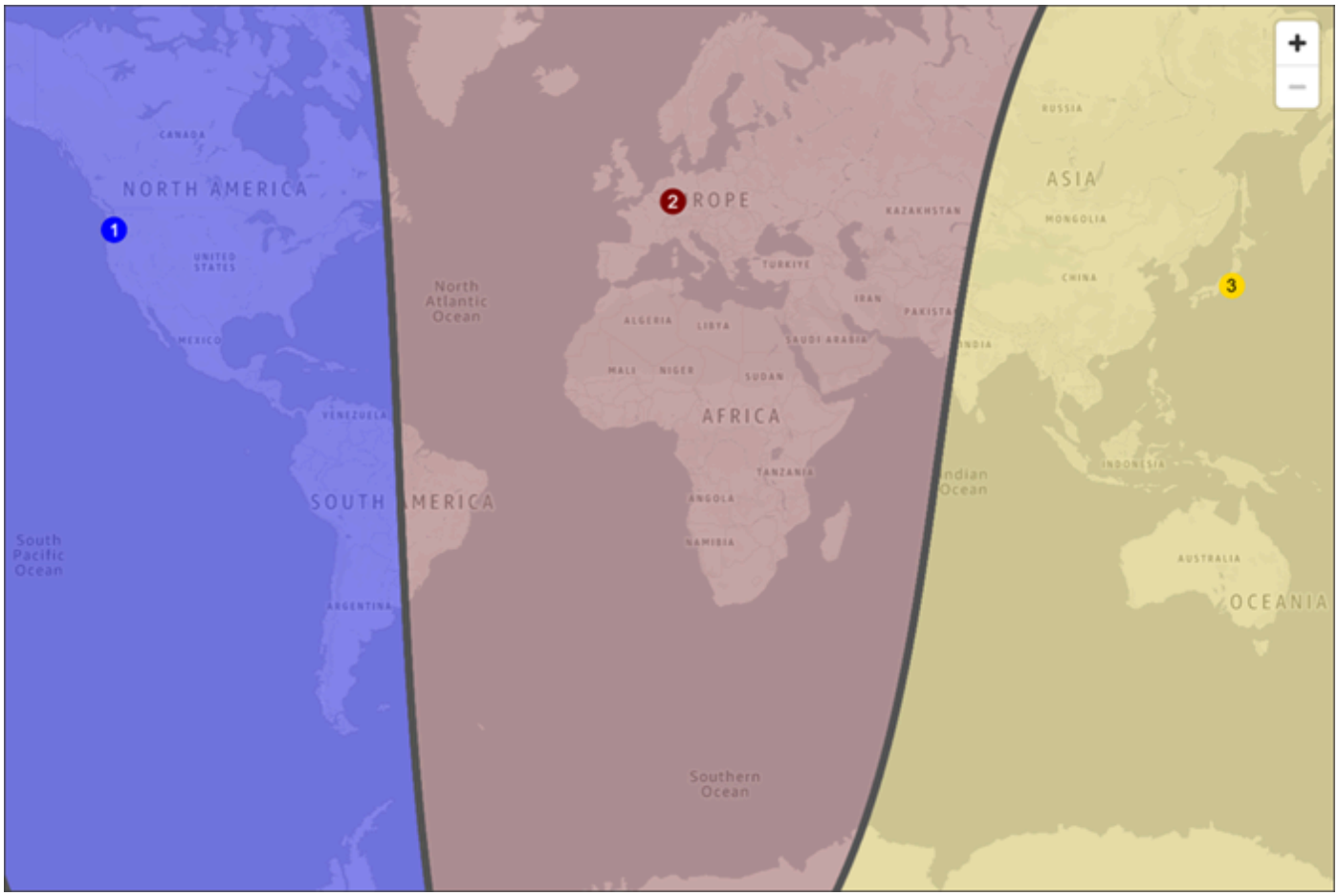
> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Sie können eine Karte anzeigen, auf der die Auswirkungen Ihrer aktuellen Einstellungen für geografische Nähe dargestellt werden. Wenn Sie beispielsweise Ressourcen in den Regionen USA West (Oregon), Europa (Frankfurt) und Asien-Pazifik (Tokio) haben und keinen Bias-Wert angeben, kann die Karte wie folgt aussehen.



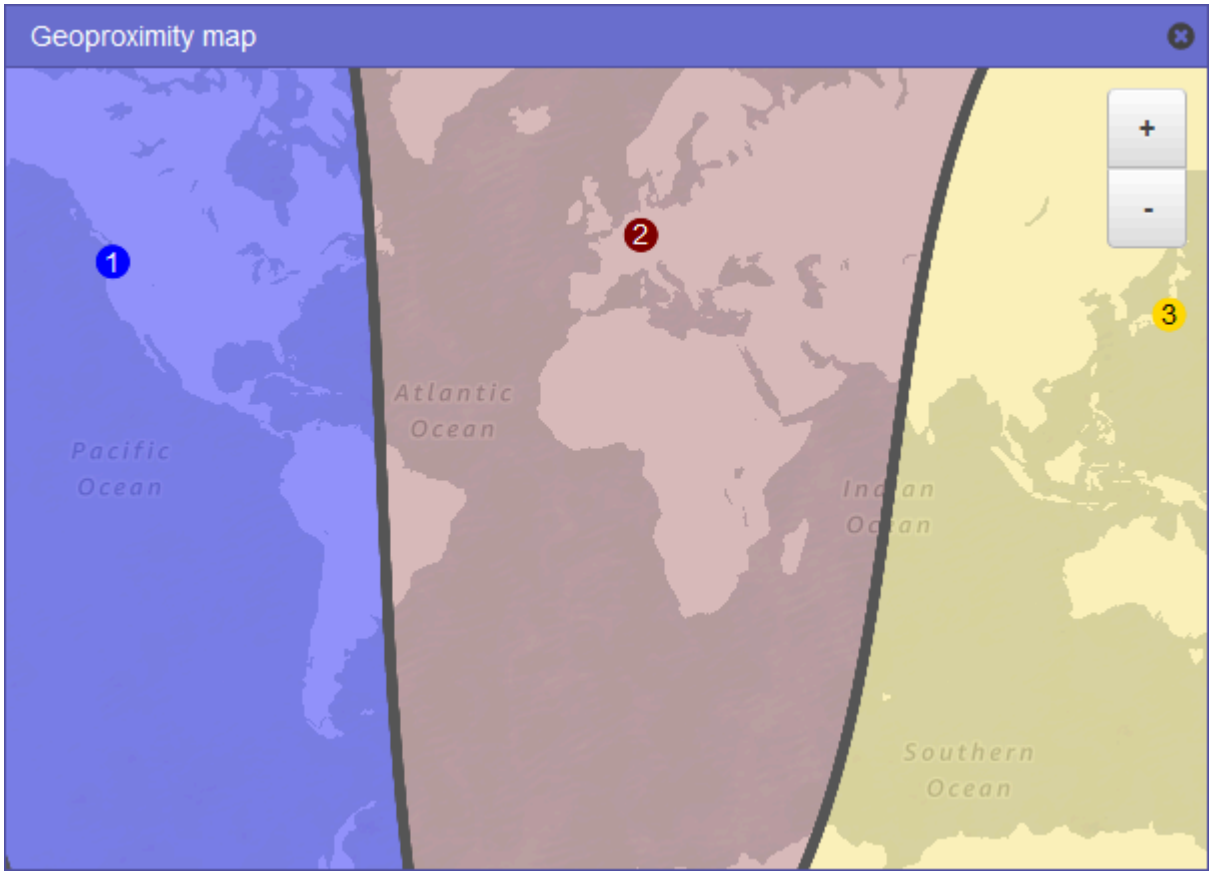
Die Karte für eine Geoproximitätsregel wird automatisch in den Eigenschaften angezeigt und aktualisiert, wenn Sie Regionen hinzufügen oder löschen.

Beachten Sie Folgendes:

- Die Karte ist bis zu etwa 10 Meilen (16 Kilometer) genau.
- Die Karte passt sich automatisch an, wenn Sie Regionen hinzufügen, bearbeiten oder löschen oder die Bias-Einstellung für eine Region ändern.
- Die Nummern und Farben der Regionen in den einzelnen Regeldefinitionen entsprechen den Nummern und Farben auf der Karte.
- Sie können die Ansicht vergrößern und verkleinern, um mehr oder weniger Details zu sehen. Sie können die Vergrößerung mit den Schaltflächen + und – auf der Karte, mit einem Touchpad oder mit dem Mausrad ändern. Wenn Sie die Region oder die Regionsnummer nicht sehen, können Sie den Eigenschaftenbereich vergrößern. Sie werden dann angezeigt.
- Sie können die Karte innerhalb des Kartenfensters verschieben, um bestimmte Bereich anzuzeigen. Verwenden Sie dazu ein Touchpad oder klicken Sie mit der Maus auf die Karte und ziehen Sie sie. Sie können auch das Kartenfenster in einem Browser-Fenster verschieben.
- Wenn sich in einer Richtlinie mehr als eine Regel für geografische Nähe befindet, können Sie die Karte für nur jeweils eine Regel anzeigen.

Old console

Sie können eine Karte anzeigen, auf der die Auswirkungen Ihrer aktuellen Einstellungen für geografische Nähe dargestellt werden. Wenn Sie beispielsweise Ressourcen in den Regionen USA West (Oregon), Europa (Frankfurt) und Asien-Pazifik (Tokio) haben und keinen Bias-Wert angeben, kann die Karte wie folgt aussehen.



Um die Karte für eine Regel für geografische Nähe anzuzeigen, wählen Sie das Grafiksymbol neben Show geoproximity map (Geoproximitätskarte anzeigen) aus. (Dieses Symbol wird über der Regel angezeigt.) Um die Karte auszublenden, wählen Sie das Symbol erneut oder wählen Sie das x rechts oben auf der Karte.

Beachten Sie Folgendes:

- Die Karte ist bis zu etwa 10 Meilen (16 Kilometer) genau.
- Die Karte passt sich automatisch an, wenn Sie Regionen hinzufügen, bearbeiten oder löschen oder die Bias-Einstellung für eine Region ändern.
- Die Nummern und Farben der Regionen in den einzelnen Regeldefinitionen entsprechen den Nummern und Farben auf der Karte.
- Sie können die Ansicht vergrößern und verkleinern, um mehr oder weniger Details zu sehen. Sie können die Vergrößerung mit den Schaltflächen + und – auf der Karte, mit einem Touchpad oder mit dem Mausrad ändern.

- Sie können die Karte innerhalb des Kartenfensters verschieben, um bestimmte Bereich anzuzeigen. Verwenden Sie dazu ein Touchpad oder klicken Sie mit der Maus auf die Karte und ziehen Sie sie. Sie können auch das Kartenfenster in einem Browser-Fenster verschieben.
- Wenn sich in einer Richtlinie mehr als eine Regel für geografische Nähe befindet, können Sie die Karte für nur jeweils eine Regel anzeigen.

Erstellen zusätzlicher Versionen einer Datenverkehrsrichtlinie

Beim Bearbeiten einer Datenverkehrsrichtlinie erstellt Amazon Route 53 automatisch eine weitere Version der Datenverkehrsrichtlinie und behält die vorherige Version bei, es sei denn, Sie löschen sie. Die neue Version hat den gleichen Namen wie die Datenverkehrsrichtlinie, die Sie gerade bearbeiten; sie unterscheidet sich von der Originalversion durch eine Versionsnummer, die Route 53 automatisch schrittweise erhöht. Sie können die neue Version einer Datenverkehrsrichtlinie auf einer beliebigen vorhandenen Version einer Datenverkehrsrichtlinie mit demselben Namen basieren.

Route 53 verwendet Versionsnummern für neue Versionen einer bestimmten Datenverkehrsrichtlinie nicht wieder. Wenn Sie beispielsweise drei Versionen von erstellen MyTrafficPolicy, die letzten beiden Versionen löschen und dann eine weitere Version erstellen, ist die neue Version Version 4. Durch das Beibehalten der vorherigen Versionen stellt Route 53 sicher, dass Sie eine frühere Konfiguration wiederherstellen können, wenn eine neue Konfiguration den Datenverkehr nicht wie gewünscht weiterleitet.

Um eine neue Version einer Datenverkehrsrichtlinie zu erstellen, führen Sie die folgenden Schritte aus.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So erstellen Sie eine andere Version einer Datenverkehrsrichtlinie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den Namen der Datenverkehrsrichtlinie aus, von der Sie eine neue Version erstellen möchten.
4. Aktivieren Sie in der Tabelle Traffic policy versions oben auf der Seite das Kontrollkästchen für die Datenverkehrsrichtlinien-Version, die Sie als Basis für die neue Datenverkehrsrichtlinie verwenden möchten.
5. Wählen Sie Edit policy as new version.
6. Geben Sie im Dialogfeld Richtlinie als neue Version bearbeiten eine Beschreibung für die neue Version der Verkehrsrichtlinie ein. Wir empfehlen, dass Sie eine Beschreibung angeben, um diese Version von anderen Versionen derselben Datenverkehrsrichtlinie zu unterscheiden. Wenn Sie eine neue Richtlinie erstellen, wird der Wert, den Sie angeben, in der Liste der verfügbaren Versionen für diese Datenverkehrsrichtlinie angezeigt.
7. Wählen Sie Weiter aus.
8. Aktualisieren Sie die Konfiguration nach Bedarf. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

   Sie können Regeln, Endpunkte und Verzweigungen einer Datenverkehrsrichtlinie auf folgende Weise löschen:

   - Um eine Regel oder einen Endpunkt zu löschen, wählen Sie ihn im Editor aus und klicken Sie dann im Eigenschaftenbereich auf Löschen.

     > **Important**
     >
     > Wenn Sie eine Regel löschen, die untergeordnete Regeln und Endpunkte hat, löscht Route 53 auch alle untergeordneten Elemente.

   - Wenn Sie zwei Regeln mit derselben untergeordneten Regel oder demselben untergeordneten Endpunkt verbinden und eine der Verbindungen löschen möchten, wählen Sie die Verbindung aus, die Sie löschen möchten, und klicken Sie dann im Eigenschaftenbereich auf Löschen.

9. Wenn Sie die Bearbeitung abgeschlossen haben, wählen Sie Save as new version.
10. Optional: Geben Sie die Einstellungen zum Erstellen von einer oder mehreren Richtliniendatensätzen in einer gehosteten Zone unter Verwendung der neuen Datenverkehrsrichtlinien-Version an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben. Darüber hinaus können Sie Richtliniendatensätze zu einem späteren Zeitpunkt erstellen, entweder in derselben gehosteten -Zone oder in zusätzlichen gehosteten Zonen.

    Wenn Sie jetzt keine Richtlinieneinträge erstellen möchten, wählen Sie Abbrechen. In der Konsole wird dann die Liste der Verkehrsrichtlinien und Richtliniendatensätze angezeigt, die Sie mit dem aktuellen AWS Konto erstellt haben.
11. Wenn Sie im vorhergehenden Schritt angegebenen Einstellungen für Richtliniendatensätze angegeben haben, wählen Sie Create policy record.

Old console

So erstellen Sie eine andere Version einer Datenverkehrsrichtlinie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den Namen der Datenverkehrsrichtlinie aus, von der Sie eine neue Version erstellen möchten.
4. Aktivieren Sie in der Tabelle Traffic policy versions oben auf der Seite das Kontrollkästchen für die Datenverkehrsrichtlinien-Version, die Sie als Basis für die neue Datenverkehrsrichtlinie verwenden möchten.
5. Wählen Sie Edit policy as new version.
6. Geben Sie auf der Seite Update description (Beschreibung aktualisieren) eine Beschreibung für die neue Datenverkehrsrichtlinien-Version ein. Wir empfehlen, dass Sie eine Beschreibung angeben, um diese Version von anderen Versionen derselben Datenverkehrsrichtlinie zu unterscheiden. Wenn Sie eine neue Richtlinie erstellen, wird der Wert, den Sie angeben, in der Liste der verfügbaren Versionen für diese Datenverkehrsrichtlinie angezeigt.
7. Wählen Sie Weiter aus.

8. Aktualisieren Sie die Konfiguration nach Bedarf. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

   Sie können Regeln, Endpunkte und Verzweigungen einer Datenverkehrsrichtlinie auf folgende Weise löschen:

   - Um eine Regel oder einen Endpunkt zu löschen, klicken Sie auf das x in der rechten oberen Ecke der Konsole

     > **Important**
     >
     > Wenn Sie eine Regel löschen, die untergeordnete Regeln und Endpunkte hat, löscht Route 53 auch alle untergeordneten Elemente.

   - Wenn Sie zwei Regeln mit derselben untergeordneten Regel oder einem Endpunkt verbinden und eine der Verbindungen löschen möchten, zeigen Sie mit dem Mauszeiger auf die Verbindung, die Sie löschen möchten, und klicken Sie auf das x für diese Verbindung.
9. Wenn Sie die Bearbeitung abgeschlossen haben, wählen Sie Save as new version.
10. Optional: Geben Sie die Einstellungen zum Erstellen von einer oder mehreren Richtliniendatensätzen in einer gehosteten Zone unter Verwendung der neuen Datenverkehrsrichtlinien-Version an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben. Darüber hinaus können Sie Richtliniendatensätze zu einem späteren Zeitpunkt erstellen, entweder in derselben gehosteten -Zone oder in zusätzlichen gehosteten Zonen.

    Wenn Sie jetzt keine Richtlinieneinträge erstellen möchten, wählen Sie „Diesen Schritt überspringen“. In der Konsole wird dann die Liste der Verkehrsrichtlinien und Richtliniendatensätze angezeigt, die Sie mit dem aktuellen AWS Konto erstellt haben.
11. Wenn Sie im vorhergehenden Schritt angegebenen Einstellungen für Richtliniendatensätze angegeben haben, wählen Sie Create policy record.

Erstellen einer Verkehrsrichtlinie mithilfe eines JSON-Dokuments

Sie können eine neue Datenverkehrsrichtlinie oder eine neue Version einer vorhandenen Datenverkehrsrichtlinie durch Importieren eines Dokuments im JSON-Format erstellen, das alle Endpunkte und Regeln beschreibt, die Sie in die Datenverkehrsrichtlinie aufnehmen möchten.

Weitere Informationen über das Format des JSON-Dokuments und mehrere Beispiele, die Sie kopieren und überarbeiten können, finden Sie unter Dokumentformat für Datenverkehrsrichtlinien in der Amazon-Route-53-API-Referenz.

Der einfachste Weg, das Dokument im JSON-Format für eine bestehende Version der Verkehrsrichtlinie abzurufen, besteht darin, den `get-traffic-policy` Befehl in der CLI zu verwenden. AWS Weitere Informationen finden Sie unter get-traffic-policy in der Referenz zum AWS CLI -Befehl.

Die mit dem Befehl `get-traffic-policy` erstellte JSON-Datei enthält umgekehrte Schrägstriche (\) als Escapezeichen. Bevor Sie die JSON-Datei importieren, ersetzen Sie alle umgekehrten Schrägstriche durch Nullzeichen.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So erstellen Sie eine Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Um eine neue Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments zu erstellen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Navigationsbereich Traffic policies aus.
   b. Klicken Sie auf Create traffic policy.
   c. Geben Sie auf der Seite Name policy die entsprechenden Werte an. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

d. Fahren Sie mit Schritt 4 fort.

3. Um eine neue Version einer vorhandenen Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments zu erstellen, führen Sie die folgenden Schritte aus:

   a. Wählen Sie im Navigationsbereich Traffic policies aus.

   b. Wählen Sie den Namen der Datenverkehrsrichtlinie aus, auf der Sie die neue Version basieren möchten.

   c. Aktivieren Sie in der Tabelle Traffic policy versions das Kontrollkästchen für die Version, auf der Sie die neue Version basieren möchten.

   d. Wählen Sie Edit policy as new version.

   e. Geben Sie auf der Seite Update description (Beschreibung aktualisieren) eine Beschreibung für die neue Version ein.

   f. Fahren Sie mit Schritt 4 fort.

4. Wählen Sie Weiter aus.

5. Wählen Sie auf der Editor-Seite das JSON-Editor-Symbol

   ()

   in der oberen rechten Ecke des Editors aus.

6. Geben Sie eine neue Datenverkehrsrichtlinie, fügen Sie eine Beispiel-Datenverkehrsrichtlinie ein oder fügen Sie eine vorhandene Datenverkehrsrichtlinie ein.

   Beispiele für Richtlinien finden Sie unter JSON-Beispiele für Traffic Flow-Richtlinien.

7. Wählen Sie Aktualisieren aus.

Old console

So erstellen Sie eine Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

2. Um eine neue Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments zu erstellen, führen Sie die folgenden Schritte aus:

   a. Wählen Sie im Navigationsbereich Traffic policies aus.

   b. Klicken Sie auf Create traffic policy.

c. Geben Sie auf der Seite Name policy die entsprechenden Werte an. Weitere Informationen finden Sie unter Angegebene Werte beim Erstellen einer Datenverkehrsrichtlinie.

d. Fahren Sie mit Schritt 4 fort.

3. Um eine neue Version einer vorhandenen Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments zu erstellen, führen Sie die folgenden Schritte aus:

   a. Wählen Sie im Navigationsbereich Traffic policies aus.

   b. Wählen Sie den Namen der Datenverkehrsrichtlinie aus, auf der Sie die neue Version basieren möchten.

   c. Aktivieren Sie in der Tabelle Traffic policy versions das Kontrollkästchen für die Version, auf der Sie die neue Version basieren möchten.

   d. Wählen Sie Edit policy as new version.

   e. Geben Sie auf der Seite Update description (Beschreibung aktualisieren) eine Beschreibung für die neue Version ein.

   f. Fahren Sie mit Schritt 4 fort.

4. Wählen Sie Weiter aus.
5. Klicken Sie auf Import traffic policy.
6. Geben Sie eine neue Datenverkehrsrichtlinie, fügen Sie eine Beispiel-Datenverkehrsrichtlinie ein oder fügen Sie eine vorhandene Datenverkehrsrichtlinie ein.

   Beispiele für Richtlinien finden Sie unter JSON-Beispiele für Traffic Flow-Richtlinien

7. Klicken Sie auf Import traffic policy.

Anzeigen von Datenverkehrsrichtlinien-Versionen und den zugehörigen Richtliniendatensätzen

Sie können alle Versionen anzeigen, die Sie für eine Datenverkehrsrichtlinie erstellt haben, sowie alle Richtliniendatensätze, die Sie anhand der einzelnen Versionen der Datenverkehrsrichtlinie erstellt haben.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So zeigen Sie Datenverkehrsrichtlinien-Versionen und die zugehörigen Richtliniendatensätze an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den verknüpften Namen einer Verkehrsrichtlinie.
4. Die obere Tabelle listet alle Versionen auf, die Sie von einer Datenverkehrsrichtlinie erstellt haben. Die Tabelle enthält die folgenden Informationen:

   Versionsnummer:

   Die Nummer jeder einzelnen Version einer Datenverkehrsrichtlinie, die Sie erstellt haben. Wenn Sie die Versionsnummer auswählen, zeigt die Konsole die Konfiguration für diese Version an.

   Anzahl der Richtliniendatensätze

   Die Anzahl der Richtliniendatensätze, die Sie mithilfe dieser Datenverkehrsrichtlinien-Version erstellt haben.

   DNS-Typ

   Der DNS-Typ, den Sie beim Erstellen der Datenverkehrsrichtlinien-Version angegeben haben.

Versionsbeschreibungen

Die Beschreibung, die Sie beim Erstellen der Datenverkehrsrichtlinien-Version angegeben haben.

5. Die untere Tabelle listet alle Richtliniendatensätze auf, die Sie mithilfe der Datenverkehrsrichtlinien-Versionen in der oberen Tabelle erstellt haben. Die Tabelle enthält die folgenden Informationen:

   DNS-Name

   Die DNS-Namen, die Sie der Datenverkehrsrichtlinie zugeordnet haben.

   Status

   Die folgenden Werte sind möglich:

   Angewandt

   Route 53 hat das Erstellen oder Aktualisieren eines Richtliniendatensatzes und der zugehörigen Datensätze beendet.

   Erstellen

   Route 53 erstellt Datensätze für einen neuen Richtliniendatensatz.

   Aktualisieren

   Sie haben einen Datensatz aktualisiert und Route 53 ist beim Erstellen einer neuen Gruppe von Datensätzen, die die vorhandene Gruppe von Ressourcendatensätzen für den angegebenen DNS-Namen ersetzen.

   Löschen

   Route 53 ist dabei, einen Richtliniendatensatz und die zugehörigen Datensätze zu löschen.

   Fehlgeschlagen

   Route 53 konnte den Richtliniendatensatz und die zugehörigen Datensätze nicht erstellen oder aktualisieren.

   DNS-Typ

   Der DNS-Typ von allen Datensätzen, die Route 53 für diesen Richtliniendatensatz erstellt hat. Wenn Sie einen Richtliniendatensatz bearbeiten, müssen Sie eine

Datenverkehrsrichtlinien-Version angeben, die denselben DNS-Typ wie der Richtliniendatensatz hat, den Sie gerade bearbeiten.

Version

Gibt die Version der Datenverkehrsrichtlinie an, die Sie verwendet haben, um den Richtliniendatensatz zu erstellen.

TTL (in Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Wenn Sie eine längere Dauer eingeben (beispielsweise 172 800 Sekunden oder zwei Tage), bezahlen Sie eine geringere Gebühr für Route 53, da die rekursiven Resolver weniger häufig Anforderungen an Route 53 senden. Es dauert allerdings länger, bis Änderungen an Datensätzen (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern.

Old console

So zeigen Sie Datenverkehrsrichtlinien-Versionen und die zugehörigen Richtliniendatensätze an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den Namen einer Datenverkehrsrichtlinie aus.
4. Die obere Tabelle listet alle Versionen auf, die Sie von einer Datenverkehrsrichtlinie erstellt haben. Die Tabelle enthält die folgenden Informationen:

   Versionsnummer:

   Die Nummer jeder einzelnen Version einer Datenverkehrsrichtlinie, die Sie erstellt haben. Wenn Sie die Versionsnummer auswählen, zeigt die Konsole die Konfiguration für diese Version an.

   Anzahl der Richtliniendatensätze

   Die Anzahl der Richtliniendatensätze, die Sie mithilfe dieser Datenverkehrsrichtlinien-Version erstellt haben.

DNS-Typ

Der DNS-Typ, den Sie beim Erstellen der Datenverkehrsrichtlinien-Version angegeben haben.

Versionsbeschreibung

Die Beschreibung, die Sie beim Erstellen der Datenverkehrsrichtlinien-Version angegeben haben.

5. Die untere Tabelle listet alle Richtliniendatensätze auf, die Sie mithilfe der Datenverkehrsrichtlinien-Versionen in der oberen Tabelle erstellt haben. Die Tabelle enthält die folgenden Informationen:

   DNS-Name des Richtliniendatensatzes

   Die DNS-Namen, die Sie der Datenverkehrsrichtlinie zugeordnet haben.

   Status

   Die folgenden Werte sind möglich:

   Angewandt

   Route 53 hat das Erstellen oder Aktualisieren eines Richtliniendatensatzes und der zugehörigen Datensätze beendet.

   Erstellen

   Route 53 erstellt Datensätze für einen neuen Richtliniendatensatz.

   Aktualisieren

   Sie haben einen Datensatz aktualisiert und Route 53 ist beim Erstellen einer neuen Gruppe von Datensätzen, die die vorhandene Gruppe von Ressourcendatensätzen für den angegebenen DNS-Namen ersetzen.

   Löschen

   Route 53 ist dabei, einen Richtliniendatensatz und die zugehörigen Datensätze zu löschen.

   Fehlgeschlagen

   Route 53 konnte den Richtliniendatensatz und die zugehörigen Datensätze nicht erstellen oder aktualisieren.

Verwendete Version

Gibt die Version der Datenverkehrsrichtlinie an, die Sie verwendet haben, um den Richtliniendatensatz zu erstellen.

DNS-Typ

Der DNS-Typ von allen Datensätzen, die Route 53 für diesen Richtliniendatensatz erstellt hat. Wenn Sie einen Richtliniendatensatz bearbeiten, müssen Sie eine Datenverkehrsrichtlinien-Version angeben, die denselben DNS-Typ wie der Richtliniendatensatz hat, den Sie gerade bearbeiten.

TTL (in Sekunden)

Der Zeitraum (in Sekunden), für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Wenn Sie eine längere Dauer eingeben (beispielsweise 172 800 Sekunden oder zwei Tage), bezahlen Sie eine geringere Gebühr für Route 53, da die rekursiven Resolver weniger häufig Anforderungen an Route 53 senden. Es dauert allerdings länger, bis Änderungen an Datensätzen (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern.

Löschen von Datenverkehrsrichtlinien-Versionen und Datenverkehrsrichtlinien

Um eine Datenverkehrsrichtlinie zu löschen, müssen Sie alle Versionen (einschließlich der ursprünglichen) löschen, die Sie für die Datenverkehrsrichtlinie erstellt haben. Darüber hinaus müssen Sie zum Löschen einer Datenverkehrsrichtlinien-Version alle Richtliniendatensätze löschen, die Sie mithilfe der Datenverkehrsrichtlinien-Version erstellt haben.

Important

Wenn Sie Richtliniendatensätze löschen, die Amazon Route 53 verwendet, um DNS-Abfragen zu beantworten, antwortet Route 53 nicht mehr auf Abfragen für die entsprechenden DNS-Namen. Wenn beispielsweise Route 53 den Richtliniendatensatz für www.example.com verwendet, um auf DNS-Abfragen für www.example.com zu antworten,

und Sie löschen den Richtliniendatensatz, haben Ihre Benutzer keinen Zugriff mehr auf Ihre Website oder die Webanwendung über den Domänenamen „www.example.com“.

Um Datenverkehrsrichtlinien-Versionen und optional eine Datenverkehrsrichtlinie zu löschen, führen Sie die folgenden Schritte aus:

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So löschen Sie Datenverkehrsrichtlinien-Versionen und Datenverkehrsrichtlinien

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den verknüpften Namen der Verkehrsrichtlinie aus, für die Sie Versionen der Verkehrsrichtlinien löschen möchten und die Sie optional vollständig löschen möchten.
4. Wenn die Versionen der Verkehrsrichtlinien, die Sie in der oberen Tabelle löschen möchten, in der Spalte Version der Tabelle mit den Richtlinieneinträgen angezeigt werden, aktivieren Sie die Kontrollkästchen für die entsprechenden Richtlinieneinträge in der unteren Tabelle.

   Wenn Sie beispielsweise Version 3 einer Datenverkehrsrichtlinie löschen möchten, jedoch eine der Richtliniendatensätze in der Tabelle unten mit Version 3 erstellt haben, aktivieren Sie das Kontrollkästchen für den betreffenden Richtliniendatensatz.
5. Wählen Sie Richtlinieneinträge löschen und wählen Sie im Dialogfeld Richtlinieneintrag löschen die Option Bestätigen aus.

6. Aktualisieren Sie die Seite, bis die gelöschten Richtlinieneinträge nicht mehr in der Tabelle angezeigt werden.
7. Aktivieren Sie in der oberen Tabelle die Kontrollkästchen für die Datenverkehrsrichtlinien-Versionen, die Sie löschen möchten.
8. Wählen Sie Löschen aus.
9. Wenn Sie im vorherigen Schritt alle Versionen der Verkehrsrichtlinie gelöscht haben und auch die Verkehrsrichtlinie löschen möchten, aktualisieren Sie die Seite, um die Anzeige zu aktualisieren, bis die Tabelle leer ist.
10. Wählen Sie im Navigationsbereich Traffic policies aus.
11. Aktivieren Sie in der Liste der Datenverkehrsrichtlinien das Kontrollkästchen für die Datenverkehrsrichtlinie, die Sie löschen möchten.
12. Klicken Sie auf Delete traffic policy.

Old console

So löschen Sie Datenverkehrsrichtlinien-Versionen und Datenverkehrsrichtlinien

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Traffic policies aus.
3. Wählen Sie den Namen der Datenverkehrsrichtlinie aus, für die Sie Datenverkehrsrichtlinien-Versionen löschen möchten, oder die Sie (optional) komplett löschen möchten.
4. Wenn die Datenverkehrsrichtlinien-Versionen, die Sie in der oberen Tabelle löschen möchten, in der Spalte Version used unten in der Tabelle angezeigt werden, aktivieren Sie die Kontrollkästchen für die entsprechenden Richtliniendatensätze in der unteren Tabelle.

   Wenn Sie beispielsweise Version 3 einer Datenverkehrsrichtlinie löschen möchten, jedoch eine der Richtliniendatensätze in der Tabelle unten mit Version 3 erstellt haben, aktivieren Sie das Kontrollkästchen für den betreffenden Richtliniendatensatz.
5. Klicken Sie auf Delete policy records.
6. Verwenden Sie die Aktualisierungsschaltfläche für die untere Tabelle, um die Anzeige zu aktualisieren, bis die Richtliniendatensätze, die Sie gelöscht haben, nicht mehr in der Tabelle angezeigt werden.
7. Aktivieren Sie in der oberen Tabelle die Kontrollkästchen für die Datenverkehrsrichtlinien-Versionen, die Sie löschen möchten.

8. Klicken Sie auf Delete version.
9. Wenn Sie alle Datenverkehrsrichtlinien-Versionen im vorhergehenden Schritt gelöscht haben und die Datenverkehrsrichtlinie ebenfalls löschen möchten, klicken Sie auf die Aktualisierungsschaltfläche für die obere Tabelle, um die Anzeige zu aktualisieren, bis die Tabelle leer ist.
10. Wählen Sie im Navigationsbereich Traffic policies aus.
11. Aktivieren Sie in der Liste der Datenverkehrsrichtlinien das Kontrollkästchen für die Datenverkehrsrichtlinie, die Sie löschen möchten.
12. Klicken Sie auf Delete traffic policy.

Erstellen und Verwalten von Richtliniendatensätzen

Um Internetdatenverkehr an die von Ihnen bei der Erstellung einer Datenverkehrsrichtlinie angegebenen Ressourcen weiterzuleiten, erstellen Sie einen oder mehrere Richtliniendatensätze. Jeder Richtliniendatensatz identifiziert die gehostete Zone, in der Sie den Richtliniendatensatz erstellen möchten, und den Namen der Domain oder Subdomain, für die Sie den Datenverkehr weiterleiten möchten. Wenn Sie beispielsweise Datenverkehr für www.example.com weiterleiten möchten, geben Sie die ID der gehosteten Zone für die gehostete Zone "example.com" und "www.example.com" für den Policy record DNS name (DNS-Namen des Richtliniendatensatzes) an.

Wenn Sie mit der gleichen Datenverkehrsrichtlinie Datenverkehr für mehr als einen Domänen- oder Subdomänennamen weiterleiten möchten, haben Sie zwei Möglichkeiten:

- Sie können einen Richtliniendatensatz für jeden Domänen- oder Subdomänennamen erstellen.
- Sie können einen einzelnen Richtliniendatensatz und anschließend CNAME- oder Alias-Datensätze mit Bezug zu dem Richtliniendatensatz erstellen.

Wenn Sie die gleiche Datenverkehrsrichtlinie beispielsweise für example.com, example.net und example.org verwenden möchten, können Sie eine der beiden folgenden Möglichkeiten nutzen:

- Erstellen Sie jeweils einen Richtliniendatensatz pro Domäne.
- Erstellen Sie einen Richtliniendatensatz für eine der Domänen und erstellen Sie dann in den gehosteten Zonen CNAME-Datensätze für die beiden anderen Domänen. In den beiden CNAME-Datensätzen geben Sie den Datensatznamen an, für den Sie einen Richtliniendatensatz erstellt haben.

Wenn Sie die gleiche Datenverkehrsrichtlinie für eine Domäne und deren Subdomänen, wie z. B. example.com und www.example.com, verwenden möchten, können Sie für einen Namen einen Richtliniendatensatz und für alles Übrige Alias-Datensätze erstellen. So können Sie etwa einen Richtliniendatensatz für example.com erstellen und anschließend einen Alias-Datensatz für www.example.com, wobei der example.com-Datensatz dessen Alias-Ziel ist.

> **Note**
>
> Für jeden Richtliniendatensatz, den Sie erstellen, fällt eine monatliche Gebühr an. Wenn Sie die gleiche Datenverkehrsrichtlinie für mehrere Domänen- oder Subdomänennamen verwenden möchten, können Sie mithilfe von CNAME- oder Alias-Datensätzen Ihre Gebühren reduzieren:
>
> - Wenn Sie einen Richtliniendatensatz sowie einen oder mehrere CNAME-Datensätze mit Bezug zum Richtliniendatensatz erstellen, bezahlen Sie nur für den Richtliniendatensatz und für DNS-Abfragen zu den CNAME-Datensätzen.
> - Wenn Sie in der gehosteten Zone einen Richtliniendatensatz und einen oder mehrere Alias-Datensätze mit Bezug zum Richtliniendatensatz erstellen, bezahlen Sie nur für den Richtliniendatensatz und für DNS-Abfragen zu den Alias-Datensätzen.

Themen

Erstellen von Richtliniendatensätzen

Um einen Richtliniendatensatz zu erstellen, führen Sie die folgenden Schritte aus.

> **Important**
>
> Für jede Richtliniendatensatz, den Sie erstellen, fällt eine monatliche Gebühr an. Wenn Sie den Richtliniendatensatz später löschen, wird die Gebühr anteilig berechnet. Weitere Informationen finden Sie im Abschnitt „Datenverkehrsfluss“ von Amazon-Route-53-Preise.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So erstellen Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Klicken Sie auf der Seite Policy records auf Create policy records.
4. Geben Sie auf der Seite Create policy records die entsprechenden Werte an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben.
5. Um derselben Hosting-Zone weitere Einträge hinzuzufügen, wählen Sie Richtlinieneintrag hinzufügen.
6. Klicken Sie auf Create policy records.

   Es kann mehrere Minuten dauern, bis der Status des erstellten Richtliniendatensatzes als Angewendet angezeigt wird.
7. Wenn Sie Richtliniendatensätze in einer anderen gehosteten Zone erstellen möchten, wiederholen Sie die Schritte 3 bis 5.

> **Note**
>
> Wenn der Status des Richtlinieneintrags Fehlgeschlagen lautet, wählen Sie die Schaltfläche Info neben dem Status aus, um weitere Informationen zu dem Fehler zu

erhalten. Wenn Sie weitere Hilfe benötigen und den AWS Support kontaktieren möchten, finden Sie weitere Informationen unter Wie erhalte ich technischen Support von AWS?

Old console

So erstellen Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Klicken Sie auf der Seite Policy records auf Create policy records.
4. Geben Sie auf der Seite Create policy records die entsprechenden Werte an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben.
5. Klicken Sie auf Create policy records.

   Es kann mehrere Minuten dauern, bis der Status des erstellten Richtliniendatensatzes als Angewendet angezeigt wird.
6. Wenn Sie Richtliniendatensätze in einer anderen gehosteten Zone erstellen möchten, wiederholen Sie die Schritte 3 bis 5.

> **Note**
>
> Wenn der Status des Richtlinieneintrags Fehlgeschlagen lautet, wählen Sie die Schaltfläche Info neben dem Status aus, um weitere Informationen zu dem Fehler zu erhalten. Wenn Sie weitere Hilfe benötigen und den AWS Support kontaktieren möchten, finden Sie weitere Informationen unter Wie erhalte ich technischen Support von AWS?

Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden. Die folgende Liste gilt für beide Konsolen, sofern nicht anders angegeben.

Beim Erstellen oder Aktualisieren von Richtliniendatensätzen geben Sie die folgenden Werte an

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

Datenverkehrsrichtlinie

Wählen Sie die Datenverkehrsrichtlinie aus, deren Konfiguration Sie für diesen Richtliniendatensatz verwenden möchten.

Version

Wählen Sie die Version der Datenverkehrsrichtlinie aus, deren Konfiguration Sie für diesen Richtliniendatensatz verwenden möchten.

Wenn Sie einen vorhandenen Richtliniendatensatz aktualisieren, müssen Sie eine Version auswählen, deren DNS-Typ mit dem aktuellen DNS-Typ der Datensatzrichtlinie übereinstimmt. Wenn der DNS-Typ des Richtliniendatensatzes beispielsweise A ist, müssen Sie eine Version auswählen, deren DNS-Typ ebenfalls A ist.

Gehostete Zone

Wählen Sie die gehostete Zone aus, in der Sie einen Richtliniendatensatz mithilfe der angegebenen Datenverkehrsrichtlinie und Version erstellen möchten. Sie können den Wert für Hosted Zone nicht ändern, nachdem Sie einen Richtliniendatensatz erstellt haben.

DNS-Name (neue Konsole), DNS-Name des Richtlinieneintrags (alte Konsole)

Wenn Sie einen Richtliniendatensatz erstellen, geben Sie den Domänennamen oder den Subdomänennamen ein, für den Route 53 DNS-Abfragen beantworten soll, mithilfe der Konfiguration in der angegebenen Datenverkehrsrichtlinie und Version.

Um dieselbe Konfiguration für mehr als einen Domainnamen oder Subdomänennamen in der angegebenen Hosting-Zone zu verwenden, wählen Sie Richtlinieneintrag hinzufügen (neue Konsole) oder Weiteren Richtlinieneintrag hinzufügen (alte Konsole) und geben Sie den entsprechenden Domänen- oder Subdomänennamen und TTL ein.

Sie können den Wert für Policy record DNS name nicht ändern, nachdem Sie einen Richtliniendatensatz erstellt haben.

TTL (in Sekunden)

Geben Sie den Zeitraum in Sekunden ein, für den Informationen über diesen Datensatz von rekursiven DNS-Resolvern zwischengespeichert werden sollen. Wenn Sie eine längere Dauer eingeben (beispielsweise 172 800 Sekunden oder 2 Tage), bezahlen Sie eine geringere Gebühr für Route 53, da die rekursiven Resolver weniger häufig Anforderungen an Route 53 senden. Es dauert allerdings länger, bis Änderungen an Datensätzen (z. B. eine neue IP-Adresse) wirksam werden. Dies liegt daran, dass die rekursiven Resolver die Werte in ihrem Zwischenspeicher für einen längeren Zeitraum verwenden, anstatt aktuelle Informationen von Route 53 anzufordern.

Aktualisieren von Richtliniendatensätzen

Um die Einstellungen in einem Richtliniendatensatz zu aktualisieren, führen Sie die folgenden Schritte aus.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So aktualisieren Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Aktivieren Sie auf der Seite Richtliniendatensätze das Kontrollkästchen für den Richtlinieneintrag, den Sie aktualisieren möchten, und wählen Sie Bearbeiten aus.
4. Geben Sie auf der Seite Edit policy record die entsprechenden Werte an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben.
5. Wählen Sie Edit policy record.

   Es kann mehrere Minuten dauern, bis der Status des erstellten Richtliniendatensatzes als Angewendet angezeigt wird.
6. Wenn Sie einen weiteren Richtliniendatensatz aktualisieren möchten, wiederholen Sie die Schritte 3 bis 5.

> **Note**
>
> Wenn der Status des Richtlinieneintrags Fehlgeschlagen lautet, wählen Sie die Schaltfläche Info neben dem Status aus, um weitere Informationen zu dem Fehler zu erhalten. Wenn Sie weitere Hilfe benötigen und den AWS Support kontaktieren möchten, finden Sie weitere Informationen unter Wie erhalte ich technischen Support von AWS?

Old console

So aktualisieren Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Aktivieren Sie auf der Seite Policy records das Kontrollkästchen für den zu aktualisierenden Richtliniendatensatz, und wählen Sie Edit policy record.

4. Geben Sie auf der Seite Edit policy record die entsprechenden Werte an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Richtliniendatensätzen angeben.
5. Wählen Sie Edit policy record.

   Es kann mehrere Minuten dauern, bis der Status des erstellten Richtliniendatensatzes als Angewendet angezeigt wird.
6. Wenn Sie einen weiteren Richtliniendatensatz aktualisieren möchten, wiederholen Sie die Schritte 3 bis 5.

> **Note**
>
> Wenn der Status des Richtlinieneintrags Fehlgeschlagen lautet, wählen Sie die Schaltfläche Info neben dem Status aus, um weitere Informationen zu dem Fehler zu erhalten. Wenn Sie weitere Hilfe benötigen und den AWS Support kontaktieren möchten, finden Sie weitere Informationen unter Wie erhalte ich technischen Support von AWS?

Löschen von Richtliniendatensätzen

Um einen Richtliniendatensatz zu löschen, führen Sie die folgenden Schritte aus.

> **Important**
>
> Wenn Sie Richtliniendatensätze löschen, die Amazon Route 53 verwendet, um DNS-Abfragen zu beantworten, antwortet Route 53 nicht mehr auf Abfragen für die entsprechenden DNS-Namen. Wenn beispielsweise Route 53 den Richtliniendatensatz für www.example.com verwendet, um auf DNS-Abfragen für www.example.com zu antworten, und Sie löschen den Richtliniendatensatz, haben Ihre Benutzer keinen Zugriff mehr auf Ihre Website oder die Webanwendung über den Domänenamen „www.example.com“.

> **Note**
>
> Wir aktualisieren die Traffic Flow-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So löschen Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Aktivieren Sie auf der Seite Richtlinieneinträge die Kontrollkästchen für die Richtlinieneinträge, die Sie löschen möchten, und wählen Sie Löschen aus.
4. Wählen Sie im Dialogfeld Richtlinieneintrag löschen die Option Bestätigen aus.

   Warten Sie einige Minuten und aktualisieren Sie die Seite, um sicherzustellen, dass der Richtliniendatensatz nicht mehr in der Liste angezeigt wird.

Old console

So löschen Sie einen Richtliniendatensatz

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Policy records aus.
3. Aktivieren Sie auf der Seite Policy records die Kontrollkästchen für die zu löschenden Richtliniendatensätze, und wählen Sie Delete policy record.

   Warten Sie einige Minuten und aktualisieren Sie die Seite, um sicherzustellen, dass der Richtliniendatensatz nicht mehr in der Liste angezeigt wird.

Was ist Route 53 VPC Resolver?

Route 53 VPC Resolver reagiert rekursiv auf DNS-Abfragen von AWS Ressourcen für öffentliche Aufzeichnungen, Amazon VPC-spezifische DNS-Namen und private gehostete Zonen von Amazon Route 53 und ist standardmäßig in allen verfügbar. VPCs

> **Note**
>
> Route 53 VPC Resolver hieß früher Route 53 Resolver, wurde aber mit der Einführung von Route 53 Global Resolver umbenannt.

Eine Amazon VPC stellt über eine VPC+2-IP-Adresse eine Verbindung zu einem VPC-Resolver her. Diese VPC+2-Adresse stellt eine Verbindung zu einem VPC-Resolver innerhalb einer Availability Zone her.

Ein VPC-Resolver beantwortet automatisch DNS-Anfragen für:

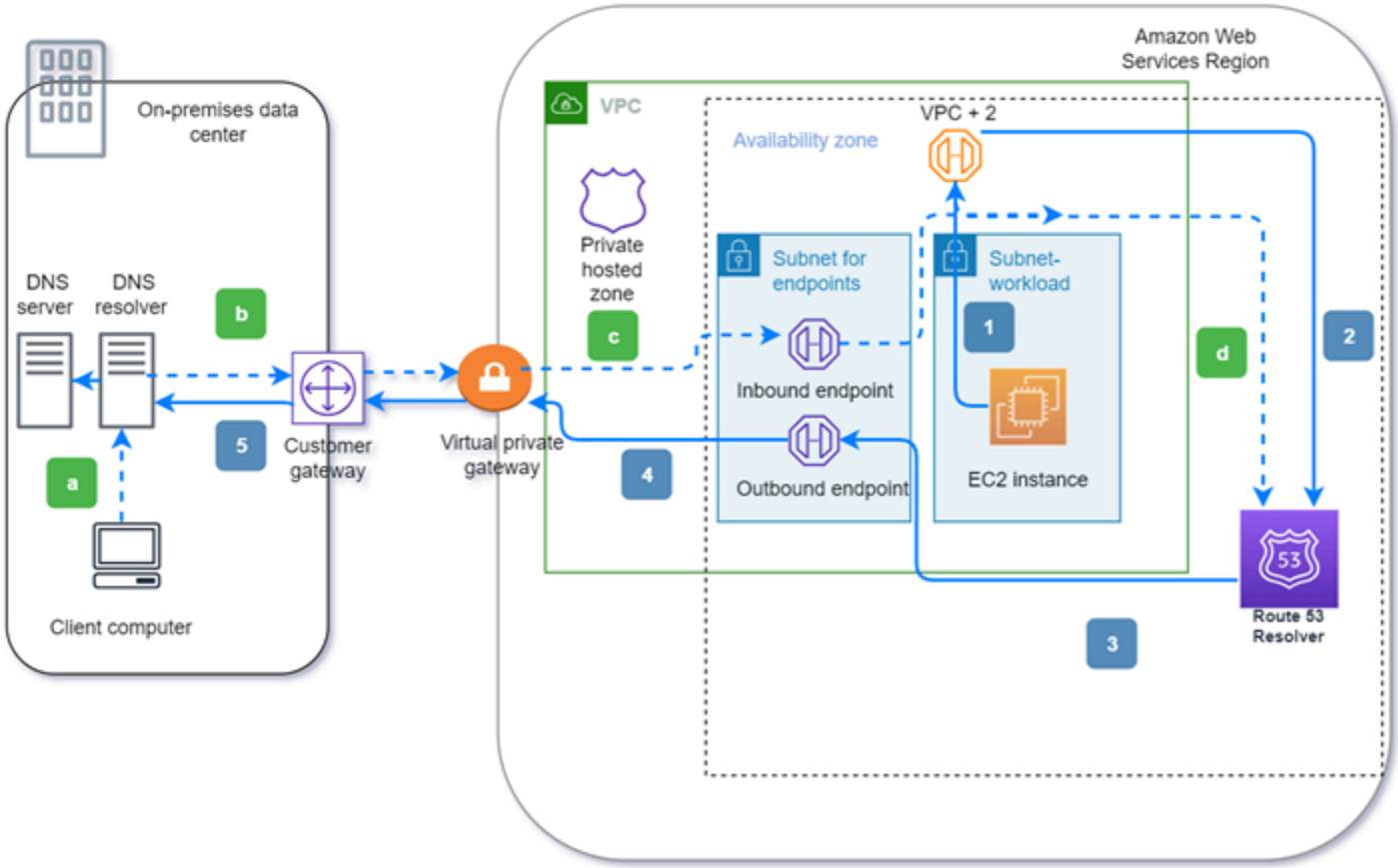
- Lokale VPC-Domainnamen für EC2 Instances (z. B. ec2-192-0-2-44.compute-1.amazonaws.com).
- Datensätze in privaten gehosteten Zonen (z. B. acme.example.com).
- Für öffentliche Domainnamen führt VPC Resolver rekursive Suchvorgänge auf öffentlichen Nameservern im Internet durch.

Wenn Sie über Workloads verfügen, die VPCs sowohl lokale als auch lokale Ressourcen nutzen, müssen Sie auch lokal gehostete DNS-Einträge auflösen. In ähnlicher Weise müssen diese lokalen Ressourcen möglicherweise Namen auflösen, die auf gehostet werden. AWS Mithilfe von Resolver-Endpunkten und bedingten Weiterleitungsregeln können Sie DNS-Abfragen zwischen Ihren lokalen Ressourcen lösen und VPCs ein Hybrid-Cloud-Setup über VPN oder Direct Connect (DX) erstellen. Das heißt:

- Eingehende Resolver-Endpunkte ermöglichen DNS-Abfragen an Ihre VPC von Ihrem On-Premises-Netzwerk oder einer anderen VPC.
- Ausgehende Resolver-Endpunkte ermöglichen DNS-Abfragen von Ihrer VPC an Ihr On-Premises-Netzwerk oder eine andere VPC.

- Mit Resolver-Regeln können Sie eine Weiterleitungsregel für alle Domainnamen erstellen und den Namen der Domain angeben, für die Sie DNS-Abfragen von Ihrer VPC an einen On-Premises-DNS-Resolver und von Ihrem On-Premises-Netzwerk an Ihre VPC weiterleiten möchten. Regeln werden direkt auf Ihre VPC angewendet und können von mehreren Konten gemeinsam genutzt werden.

Das folgende Diagramm zeigt die hybride DNS-Auflösung mit Resolver-Endpunkten. Beachten Sie, dass das Diagramm vereinfacht ist, sodass nur eine Availability Zone angezeigt wird.



Die Abbildung zeigt die folgenden Schritte:

Ausgehend (durchgezogene Pfeile 1–5):

1. Eine EC2 Amazon-Instance muss eine DNS-Anfrage an die Domain internal.example.com auflösen. Der autoritative DNS-Server befindet sich im On-Premises-Rechenzentrum. Diese DNS-Abfrage wird an die VPC+2 in der VPC gesendet, die eine Verbindung zum VPC Resolver herstellt.
2. Eine VPC Resolver-Weiterleitungsregel ist so konfiguriert, dass Abfragen an internal.example.com im lokalen Rechenzentrum weitergeleitet werden.

3. Die Abfrage wird an einen ausgehenden Endpunkt weitergeleitet.
4. Der ausgehende Endpunkt leitet die Anfrage über eine private Verbindung zwischen und dem Rechenzentrum an den lokalen DNS-Resolver weiter. AWS Die Verbindung kann entweder Direct Connect oder sein AWS Site-to-Site VPN, dargestellt als virtuelles privates Gateway.
5. Der lokale DNS-Resolver löst die DNS-Abfrage für internal.example.com auf und gibt die Antwort über denselben Pfad in umgekehrter Reihenfolge an die EC2 Amazon-Instance zurück.

Eingehend (gestrichelte Pfeile a—d):

a. Ein Client im lokalen Rechenzentrum muss eine DNS-Abfrage an eine AWS Ressource für die Domain dev.example.com auflösen. Er sendet die Abfrage an den On-Premises-DNS-Resolver.
b. Der On-Premises-DNS-Resolver verfügt über eine Weiterleitungsregel, die Abfragen an dev.example.com an einen eingehenden Endpunkt weiterleitet.
c. Die Abfrage erreicht den eingehenden Endpunkt über eine private Verbindung, z. B. Direct Connect oder AWS Site-to-Site VPN, die als virtuelles Gateway dargestellt wird.
d. Der eingehende Endpunkt sendet die Anfrage an VPC Resolver, und VPC Resolver löst die DNS-Abfrage für dev.example.com auf und gibt die Antwort über denselben Pfad in umgekehrter Reihenfolge an den Client zurück.

Themen

Auflösen von DNS-Abfragen zwischen und Ihrem Netzwerk VPCs

Der VPC Resolver enthält Endpoints, die Sie so konfigurieren, dass sie DNS-Anfragen an und von Ihrer lokalen Umgebung beantworten.

> **Note**
>
> Die Weiterleitung von privaten DNS-Abfragen an eine beliebige VPC CIDR + 2-Adresse von lokalen oder anderen VPC-DNS-Servern wird nicht unterstützt und kann zu instabilen Ergebnissen führen. Stattdessen empfehlen wir Ihnen, einen eingehenden Resolver-Endpunkt zu verwenden.

Sie können die DNS-Auflösung auch zwischen VPC-Resolver und DNS-Resolvern in Ihrem Netzwerk integrieren, indem Sie Weiterleitungsregeln konfigurieren. Ihr Netzwerk kann jedes Netzwerk umfassen, das von Ihrer VPC aus erreichbar ist, z. B. die folgenden:

- Die VPC selbst
- Eine weitere per Peering verbundene VPC
- Ein lokales Netzwerk, das AWS mit einem VPN oder einem Direct Connect NAT-Gateway (Network Address Translation) verbunden ist

Bevor Sie mit der Weiterleitung von Abfragen beginnen, erstellen Sie Resolver-Endpunkte für eingehenden und and/or ausgehenden Datenverkehr in der verbundenen VPC. Diese Endpunkte bieten einen Pfad für eingehende oder ausgehende Abfragen:

Eingehender Endpunkt: DNS-Resolver in Ihrem Netzwerk können DNS-Anfragen über diesen Endpunkt an Route 53 VPC Resolver weiterleiten

Es gibt zwei Arten von Eingangsendpunkten: einen standardmäßigen Eingangsendpunkt, der an IP-Adressen weiterleitet, und einen eingehenden Delegationsendpunkt, der die Autorität für eine Subdomain, die in der privaten Hosted Zone Route 53 gehostet wird, an den Route 53 VPC Resolver delegiert. Eingehende Endpunkte ermöglichen es Ihren DNS-Resolvern, Domainnamen für AWS Ressourcen wie EC2 Instanzen oder Datensätze in einer privaten gehosteten Route 53-Zone einfach aufzulösen. Weitere Informationen finden Sie unter Wie DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Resolver-Endpunkte weiterleiten.

Ausgehender Endpunkt: VPC Resolver leitet Anfragen über diesen Endpunkt bedingt an Resolver in Ihrem Netzwerk weiter

Zum Weiterleiten ausgewählter Abfragen erstellen Sie Resolver-Regeln, die die Domainnamen für die DNS-Abfragen angeben, die Sie weiterleiten möchten (z. B. example.com), und die IP-Adressen der DNS-Resolver in Ihrem Netzwerk, an die die Abfragen weitergeleitet werden sollen.

Wenn eine Abfrage mehreren Regeln entspricht (example.com, acme.example.com), wählt VPC Resolver die Regel mit der genauesten Übereinstimmung (acme.example.com) und leitet die Abfrage an die IP-Adressen weiter, die Sie in dieser Regel angegeben haben. Es gibt drei Arten von Regeln: Weiterleitung, System und Delegierung. Weitere Informationen finden Sie unter Wie Resolver-Endpunkte DNS-Anfragen von Ihrem an Ihr Netzwerk weiterleiten VPCs .

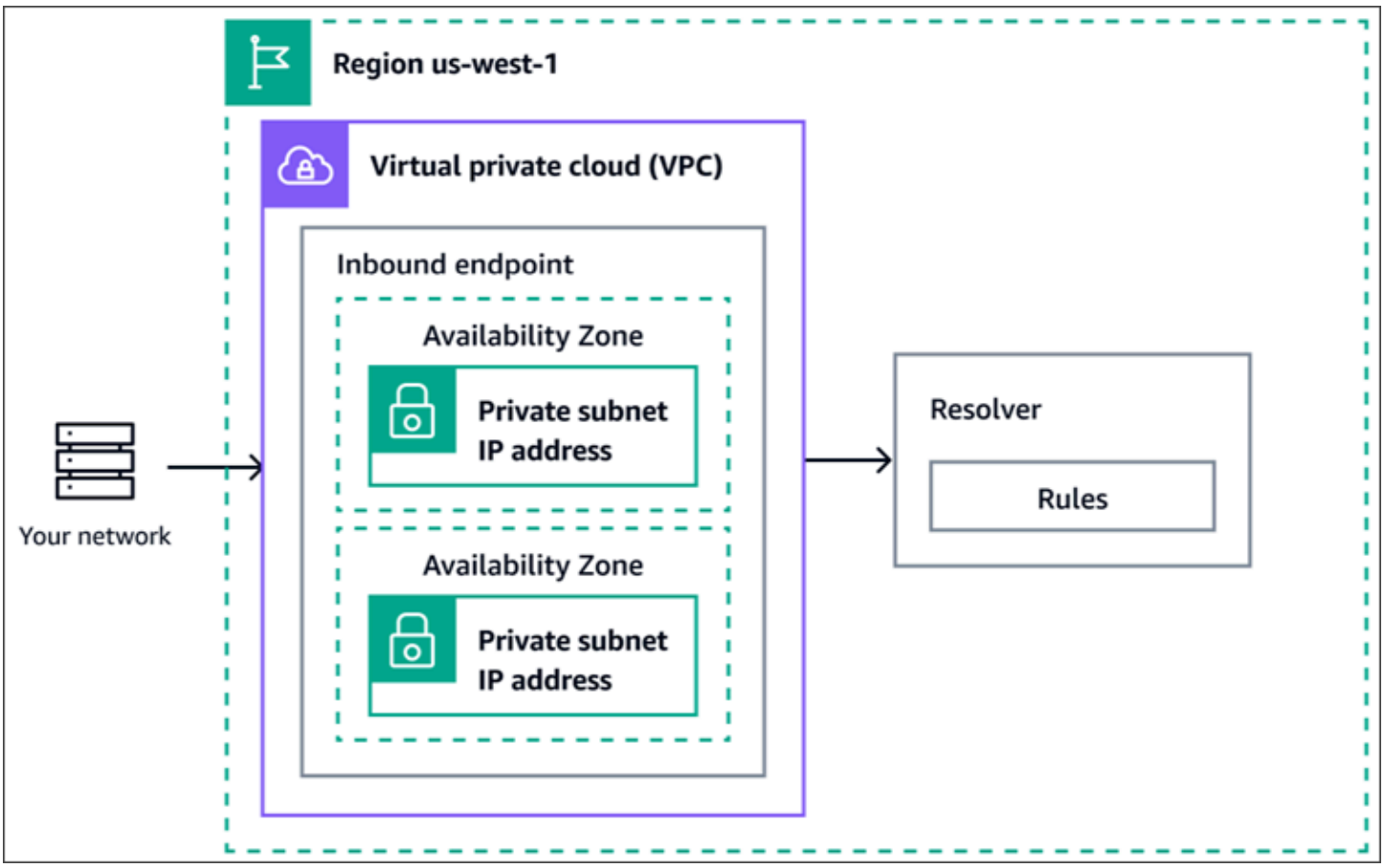
Wie Amazon VPC ist VPC Resolver regional. In jeder Region, in der Sie tätig sind VPCs, können Sie wählen, ob Sie Anfragen von Ihrem Netzwerk VPCs an Ihr Netzwerk (ausgehende Anfragen), von Ihrem Netzwerk an Ihr VPCs (eingehende Anfragen) oder beides weiterleiten möchten.

Sie können keine Resolver-Endpunkte in einer VPC erstellen, die nicht Ihnen gehört. Nur der VPC Besitzer kann Ressourcen wie eingehende Endpunkte auf VPC-Ebene erstellen.

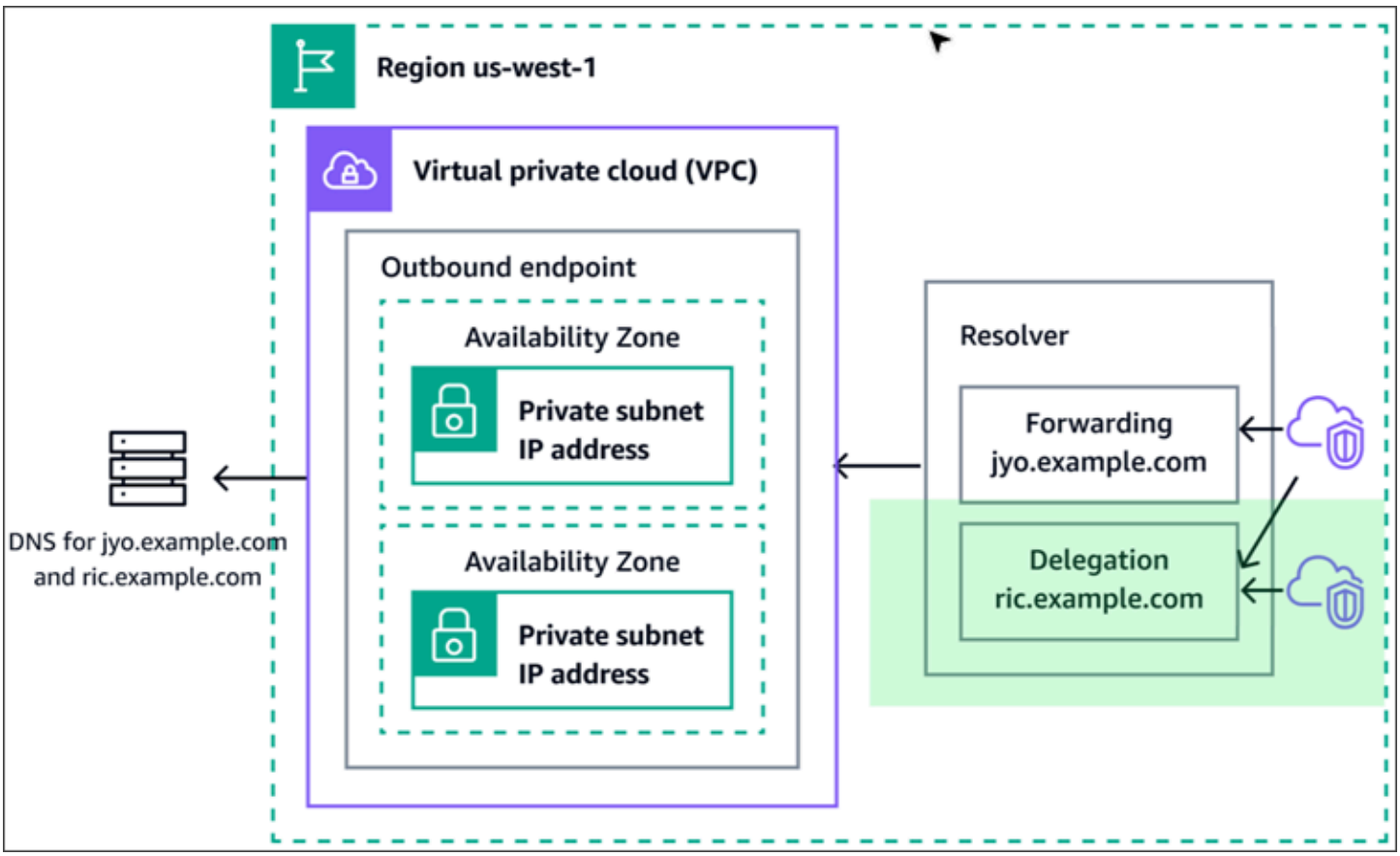
> **Note**
>
> Wenn Sie einen Resolver-Endpunkt erstellen, können Sie keine VPC angeben, für die das Instance-Tenancy-Attribut auf `dedicated` festgelegt ist. Weitere Informationen finden Sie unter .

Erstellen Sie zur Verwendung eingehender oder ausgehender Weiterleitungen einen Resolver-Endpunkt in Ihrer VPC. Im Rahmen der Definition eines Endpunkts geben Sie die IP-Adressen oder die DNS-Delegierung an, an die Sie eingehende DNS-Anfragen weiterleiten möchten, oder die IP-Adressen, von denen ausgehende Anfragen stammen sollen. Für jede IP-Adresse und Delegierung, die Sie angeben, erstellt VPC Resolver automatisch eine elastische VPC-Netzwerkschnittstelle.

Das folgende Diagramm zeigt den Pfad einer DNS-Abfrage von einem DNS-Resolver in Ihrem Netzwerk zum Route 53-Resolver an.



Das folgende Diagramm zeigt den Pfad einer DNS-Abfrage von einer EC2 Instanz in einer Ihrer Instanzen VPCs zu einem DNS-Resolver in Ihrem Netzwerk. Die Domain jyo.example.com verwendet eine Weiterleitungsregel, wohingegen die Subdomain ric.example.com die Weiterleitungsberechtigung an VPC Resolver delegiert hat.



Eine Übersicht über VPC Netzwerkschnittstellen finden Sie unterElastic Network-Schnittstelleim Amazon VPC User Guideaus.

Topics

- Wie DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Resolver-Endpunkte weiterleiten
- Wie Resolver-Endpunkte DNS-Anfragen von Ihrem an Ihr Netzwerk weiterleiten VPCs
- Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten

Wie DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Resolver-Endpunkte weiterleiten

Um DNS-Abfragen von Ihrem Netzwerk an den Route 53 VPC Resolver weiterzuleiten, erstellen Sie eingehende Endpunkte in einer Region. AWS Es gibt zwei Kategorien von Eingangsendpunkten: Standard- und Delegationsendpunkte.

Schritte zum Erstellen von Standardendpunkten für eingehenden Datenverkehr

1. Sie erstellen einen standardmäßigen Resolver-Eingangsendpunkt in einer VPC und geben die IP-Adressen an, an die die Resolver in Ihrem Netzwerk DNS-Anfragen weiterleiten, zusammen mit einer VPC-Sicherheitsgruppe, die Regeln für eingehenden Datenverkehr enthält, die den TCP- und UDP-Zugriff auf Port 53 zulassen. Anweisungen finden Sie unter Konfigurieren von Weiterleitungen eingehender Abfragen.

   Für jede IP-Adresse, die Sie für den eingehenden Endpunkt angeben, erstellt VPC Resolver eine VPC-Elastic elastic network interface in der VPC, in der Sie den eingehenden Endpunkt erstellt haben.

2. Sie konfigurieren Resolver in Ihrem Netzwerk, um DNS-Abfragen für die entsprechenden Domainnamen an die im eingehenden Endpunkt angegebenen IP-Adressen weiterzuleiten. Weitere Informationen finden Sie unter Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten.

So löst VPC Resolver DNS-Anfragen, die aus Ihrem Netzwerk stammen, über einen standardmäßigen Eingangsendpunkt auf:

1. Ein Webbrowser oder eine andere Anwendung in Ihrem Netzwerk sendet eine DNS-Anfrage für einen Domainnamen, den Sie an VPC Resolver weitergeleitet haben.
2. Ein Resolver in Ihrem Netzwerk leitet die Abfrage an die IP-Adressen in Ihrem eingehenden Endpunkt weiter.
3. Der eingehende Endpunkt leitet die Abfrage an VPC Resolver weiter.
4. VPC Resolver ruft den entsprechenden Wert für den Domainnamen in der DNS-Abfrage ab, entweder intern oder durch eine rekursive Suche auf öffentlichen Nameservern.
5. VPC Resolver gibt den Wert an den eingehenden Endpunkt zurück.
6. Der eingehende Endpunkt gibt den Wert an den Resolver in Ihrem Netzwerk zurück.
7. Der Resolver in Ihrem Netzwerk gibt den Wert an die Anwendung zurück.
8. Unter Verwendung des von VPC Resolver zurückgegebenen Werts sendet die Anwendung eine Anfrage, z. B. eine Anfrage für ein Objekt in einem Amazon S3 S3-Bucket.

Schritte zur Erstellung eingehender Delegationsendpunkte

1. Sie erstellen einen eingehenden Delegierungs-Resolver-Endpunkt in einer VPC. Anweisungen finden Sie unter Konfigurieren von Weiterleitungen eingehender Abfragen.

Für jede IP-Adresse, die Sie für den eingehenden Endpunkt angeben, erstellt VPC Resolver eine VPC-Elastic elastic network interface in der VPC, in der Sie den eingehenden Endpunkt erstellt haben.

2. Sie konfigurieren Resolver in Ihrem Netzwerk so, dass sie DNS-Abfragen für die entsprechenden Domainnamen an VPC Resolver delegieren. Für die Glue-Records müssen Sie die IP-Adressen für die eingehenden Endpunkte eingeben. Weitere Informationen finden Sie unter Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten.

So löst VPC Resolver DNS-Abfragen, die ihren Ursprung in Ihrem Netzwerk haben, über einen eingehenden Delegationsendpunkt auf:

1. Als Voraussetzung müssen Sie die Subdomain, die in der privaten Hosting-Zone gehostet wird, lokal delegieren. Da Sie die Subdomain über den Endpunkt für die eingehende Delegierung delegieren, verwenden Sie die IP-Adressen der eingehenden Endpunkte als Glue-Records für die Subdomain, die delegiert wird.

   > **Note**
   >
   > Möglicherweise müssen Sie auch die Glue-Datensätze hinzufügen, um sicherzustellen, dass die DNS-Abfrage aufgelöst werden kann. Wenn Sie eine Subdomain an Nameserver delegieren, die sich in derselben Zone wie die übergeordnete Domain befinden, sind Glue-Datensätze erforderlich.

2. Ein Webbrowser oder eine andere Anwendung in Ihrem Netzwerk sendet eine DNS-Abfrage für einen Domainnamen, den Sie an den VPC Resolver delegiert haben.
3. Ein Resolver in Ihrem Netzwerk leitet die Abfrage an die IP-Adressen in Ihrem eingehenden Endpunkt weiter.
4. Der eingehende Endpunkt delegiert die Abfrage an VPC Resolver.
5. VPC Resolver gibt die Adresse an die AWS Ressource von der privaten Hosting-Zone an den eingehenden Endpunkt zurück.
6. Der eingehende Endpunkt gibt den Wert an den Resolver in Ihrem Netzwerk zurück.
7. Der Resolver in Ihrem Netzwerk gibt den Wert an die Anwendung zurück.
8. Unter Verwendung des von VPC Resolver zurückgegebenen Werts sendet die Anwendung eine Anfrage, z. B. eine Anfrage für ein Objekt in einem Amazon S3 S3-Bucket.

Das Erstellen eines Eingangsendpunkts ändert nichts am Verhalten von VPC Resolver, sondern stellt lediglich einen Pfad von einem Standort außerhalb des AWS Netzwerks zum VPC Resolver bereit.

Wie Resolver-Endpunkte DNS-Anfragen von Ihrem an Ihr Netzwerk weiterleiten VPCs

Wenn Sie DNS-Abfragen von den EC2 Instances in einer oder mehreren VPCs in einer AWS Region an Ihr Netzwerk weiterleiten möchten, führen Sie die folgenden Schritte aus.

1. Sie erstellen einen ausgehenden Resolver-Endpunkt in einer VPC und geben mehrere Werte an:
   - Die VPC, die DNS-Abfragen auf dem Weg zu den Resolvern in Ihrem Netzwerk durchlaufen sollen.
   - Eine VPC-Sicherheitsgruppe, die Regeln für ausgehenden Datenverkehr enthält, die den TCP- und UDP-Zugriff auf Port 53 (oder den Port, den Sie für DNS-Abfragen in Ihrem Netzwerk verwenden) ermöglichen

   Für jede IP-Adresse, die Sie für den ausgehenden Endpunkt angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface in der von Ihnen angegebenen VPC. Weitere Informationen finden Sie unter Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten.
2. Sie erstellen eine oder mehrere Regeln, die die Domainnamen der DNS-Abfragen angeben, die Sie an VPC Resolver delegieren möchten, um sie weiterzuleiten, oder die VPC Resolver an Resolver in Ihrem Netzwerk weiterleiten soll. Für Weiterleitungsregeln geben Sie auch die IP-Adressen der Resolver an. Weitere Informationen finden Sie unter Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden.
3. Sie ordnen jede Regel der Regel zu, VPCs für die Sie DNS-Abfragen an Ihr Netzwerk weiterleiten möchten.

Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden

Regeln steuern, welche DNS-Anfragen der Resolver-Endpunkt an DNS-Resolver in Ihrem Netzwerk weiterleitet und welche Anfragen VPC Resolver selbst beantwortet.

Es gibt mehrere Möglichkeiten zum Kategorisieren von Regeln. Eine Möglichkeit ist die Kategorisierung nach Ersteller der Regeln:

- Automatisch definierte Regeln — VPC Resolver erstellt automatisch automatisch definierte Regeln und ordnet die Regeln Ihren zu. VPCs Die meisten dieser Regeln gelten für die AWS-spezifischen Domainnamen, für die VPC Resolver Anfragen beantwortet. Weitere Informationen finden Sie unter Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstellt.
- Benutzerdefinierte Regeln — Sie erstellen benutzerdefinierte Regeln und verknüpfen die Regeln mit. VPCs Derzeit können Sie zwei Arten von benutzerdefinierten Regeln erstellen: Regeln für bedingte Weiterleitungen, auch bekannt als Weiterleitungsregeln, und Delegierungsregeln. Weiterleitungsregeln veranlassen VPC Resolver, DNS-Anfragen von Ihnen VPCs an die IP-Adressen für DNS-Resolver in Ihrem Netzwerk weiterzuleiten.

  Wenn Sie eine Weiterleitungsregel für dieselbe Domain wie eine automatisch definierte Regel erstellen, leitet VPC Resolver Anfragen für diesen Domainnamen auf der Grundlage der Einstellungen in der Weiterleitungsregel an DNS-Resolver in Ihrem Netzwerk weiter.

  Delegierungsregeln leiten DNS-Abfragen mit den Delegierungsdatensätzen in der Delegierungsregel weiter, die mit den NS-Einträgen als Antwort auf die Resolver in Ihrem Netzwerk übereinstimmen.

Eine weitere Möglichkeit ist die Kategorisierung von Regeln nach Funktion:

- Bedingte Weiterleitungsregeln – Sie erstellen bedingte Weiterleitungsregeln (auch einfach als Weiterleitungsregeln bezeichnet), wenn Sie DNS-Abfragen für angegebene Domainnamen an DNS-Resolver in Ihrem Netzwerk weiterleiten möchten.
- Systemregeln — Systemregeln bewirken, dass VPC Resolver das in einer Weiterleitungsregel definierte Verhalten selektiv überschreibt. Wenn Sie eine Systemregel erstellen, löst VPC Resolver DNS-Abfragen für bestimmte Subdomänen auf, die andernfalls von DNS-Resolvern in Ihrem Netzwerk aufgelöst würden.

  Standardmäßig gelten Weiterleitungsregeln für einen Domainnamen und alle entsprechenden Subdomains. Wenn Sie Abfragen für eine Domain an einen Resolver in Ihrem Netzwerk weiterleiten möchten, Abfragen für einige Subdomains hingegen nicht, erstellen Sie eine Systemregel für die Subdomains. Wenn Sie beispielsweise eine Weiterleitungsregel für example.com erstellen, Abfragen für acme.example.com jedoch nicht weiterleiten möchten, erstellen Sie eine Systemregel und geben für den Domainnamen acme.example.com an.
- Rekursive Regel — VPC Resolver erstellt automatisch eine rekursive Regel mit dem Namen Internet Resolver. Diese Regel bewirkt, dass Route 53 VPC Resolver als rekursiver Resolver für alle Domainnamen fungiert, für die Sie keine benutzerdefinierten Regeln erstellt haben und für die

VPC Resolver keine automatisch definierten Regeln erstellt hat. Informationen zum Überschreiben dieses Verhaltens finden Sie unter „Weiterleiten aller Abfragen an Ihr Netzwerk“ später in diesem Thema.

Sie können benutzerdefinierte Regeln erstellen, die für bestimmte Domainnamen (Ihre oder die meisten Domainnamen), für öffentliche AWS Domainnamen oder für alle AWS Domainnamen gelten.

Weiterleiten von Abfragen für spezifische Domainnamen an Ihr Netzwerk

Um Abfragen für einen spezifischen Domainnamen wie beispielsweise example.com an Ihr Netzwerk weiterzuleiten, erstellen Sie eine Regel und geben diesen Domainnamen an. Für Weiterleitungsregeln geben Sie auch die IP-Adressen der DNS-Resolver in Ihrem Netzwerk an, an die Sie die Anfragen weiterleiten möchten, oder für Delegierungsregeln erstellen Sie den Delegierungsdatensatz, für den Sie die Autorität an lokale Resolver delegieren möchten. Anschließend ordnen Sie jede Regel der Regel zu, VPCs für die Sie DNS-Abfragen an Ihr Netzwerk weiterleiten möchten. Beispielsweise können Sie separate Regeln für example.com, example.org und example.net erstellen. Anschließend können Sie die Regeln VPCs in einer beliebigen Kombination einer AWS Region zuordnen.

Weiterleiten von Abfragen für amazonaws.com an Ihr Netzwerk

Der Domainname amazonaws.com ist der öffentliche Domainname für AWS Ressourcen wie EC2 Instances und S3-Buckets. Wenn Sie Anfragen für amazonaws.com an Ihr Netzwerk weiterleiten möchten, erstellen Sie eine Regel, geben Sie amazonaws.com als Domainnamen an und geben Sie für den Regeltyp Weiterleiten oder Delegieren an, je nachdem, welche Methode Sie verwenden möchten.

> **Note**
>
> VPC Resolver leitet DNS-Abfragen für einige Amazonaws.com-Subdomains nicht automatisch weiter, selbst wenn Sie eine Weiterleitungsregel für amazonaws.com erstellen. Weitere Informationen finden Sie unter Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstellt. Informationen zum Überschreiben dieses Verhaltens finden Sie im direkt folgenden Abschnitt „Weiterleiten aller Abfragen an Ihr Netzwerk“.

Weiterleiten aller Abfragen an Ihr Netzwerk

Wenn Sie alle Anfragen an Ihr Netzwerk weiterleiten möchten, erstellen Sie eine Regel und geben Sie „“ an. (Punkt) für den Domainnamen und ordnen Sie die Regel der Regel zu, VPCs für die Sie alle DNS-Abfragen an Ihr Netzwerk weiterleiten möchten. VPC Resolver leitet immer noch nicht alle DNS-Anfragen an Ihr Netzwerk weiter, da die Verwendung eines DNS-Resolvers außerhalb von einige Funktionen beeinträchtigen AWS würde. Beispielsweise haben einige interne AWS Domainnamen interne IP-Adressbereiche, auf die von außerhalb nicht zugegriffen werden kann. AWS Eine Liste der Domainnamen, für die Abfragen nicht an Ihr Netzwerk weitergeleitet werden, wenn Sie eine Regel für "." erstellen, finden Sie unter Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstellt.

Automatisch definierte Systemregeln für Reverse-DNS können jedoch deaktiviert werden, sodass die "."-Regel alle Reverse-DNS-Abfragen an Ihr Netzwerk weiterleiten kann. Weitere Informationen zum Deaktivieren der automatisch definierten Regeln finden Sie unter Weiterleitungsregeln für Reverse-DNS-Abfragen in VPC Resolver.

Wenn Sie versuchen möchten, DNS-Abfragen für alle Domainnamen an Ihr Netzwerk weiterzuleiten, einschließlich der Domainnamen, die standardmäßig von Weiterleitungen ausgeschlossen sind, erstellen Sie eine "."-Regel und führen Sie einen der folgenden Schritte aus:

- Legen Sie den Flag `enableDnsHostnames` für die VPC auf `false` fest.
- Erstellen Sie Regeln für die Domainnamen, die in Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstelltaufgeführt sind.

> **Important**
>
> Wenn Sie alle Domainnamen an Ihr Netzwerk weiterleiten, einschließlich der Domainnamen, die VPC Resolver ausschließt, wenn Sie eine „.“ -Regel erstellen, funktionieren einige Funktionen möglicherweise nicht mehr.

So bestimmt VPC Resolver, ob der Domainname in einer Abfrage irgendwelchen Regeln entspricht

Route 53 VPC Resolver vergleicht den Domänennamen in der DNS-Abfrage mit dem Domänennamen in den Regeln, die der VPC zugeordnet sind, von der die Abfrage stammt. VPC Resolver betrachtet die Domainnamen in den folgenden Fällen als übereinstimmend:

- Der Domainname stimmt genau überein.

- Bei dem Domainnamen in der Abfrage handelt es sich um eine Subdomain der Domain in der Regel.

Wenn der Domainname in der Regel beispielsweise acme.example.com lautet, betrachtet VPC Resolver die folgenden Domainnamen in einer DNS-Abfrage als übereinstimmend:

- acme.example.com
- zenith.acme.example.com

Bei den folgenden Domainnamen handelt es sich nicht um Übereinstimmungen:

- example.com
- nadir.example.com

Wenn der Domainname in einer Abfrage mit dem Domainnamen in mehr als einer Regel übereinstimmt (z. B. example.com und www.example.com), leitet VPC Resolver ausgehende DNS-Abfragen mit der Regel weiter, die den spezifischsten Domainnamen enthält (www.example.com).

Wie VPC Resolver bestimmt, wohin DNS-Abfragen weitergeleitet werden sollen

Wenn eine Anwendung, die auf einer EC2 Instanz in einer VPC ausgeführt wird, eine DNS-Abfrage sendet, führt Route 53 VPC Resolver die folgenden Schritte aus:

1. Resolver führt Prüfungen auf Domainnamen in Regeln aus.

   Wenn der Domänenname in einer Abfrage mit dem Domänennamen in einer Standardweiterleitungsregel übereinstimmt, leitet VPC Resolver die Abfrage an die IP-Adresse weiter, die Sie bei der Erstellung des ausgehenden Endpunkts angegeben haben. Der ausgehende Endpunkt leitet die Abfrage anschließend an die IP-Adressen von Resolvern in Ihrem Netzwerk weiter, die Sie beim Erstellen der Regel angegeben haben.

   Wenn der Delegierungsdatensatz als Antwort mit der Delegierungsregel übereinstimmt, delegiert der Resolver die Autorität über den ausgehenden Endpunkt, der der Delegierungsregel zugeordnet ist, an lokale Resolver.

   Weitere Informationen finden Sie unter So bestimmt VPC Resolver, ob der Domainname in einer Abfrage irgendwelchen Regeln entspricht.
2. Resolver Endpunkt leitet DNS-Abfragen basierend auf den Einstellungen in der "."-Regel weiter.

Wenn der Domainname in einer Abfrage nicht mit dem Domainnamen in anderen Regeln übereinstimmt, leitet VPC Resolver die Abfrage auf der Grundlage der Einstellungen im automatisch definierten Feld „“ weiter. (Punkt-) Regel. Die Punktregel gilt für alle Domainnamen mit Ausnahme einiger AWS interner Domainnamen und Datensatznamen in privaten Hosting-Zonen. Diese Regel veranlasst VPC Resolver, DNS-Anfragen an öffentliche Nameserver weiterzuleiten, wenn die Domainnamen in den Abfragen nicht mit den Namen in Ihren benutzerdefinierten Weiterleitungsregeln übereinstimmen. Wenn Sie alle Abfragen an die DNS-Resolver in Ihrem Netzwerk weiterleiten möchten, können Sie eine benutzerdefinierte Weiterleitungsregel erstellen und für den Domainnamen „.“ angeben. Wählen Sie Weiterleitung für Typ und legen Sie die IP-Adressen dieser Resolver fest.

3. VPC Resolver gibt die Antwort an die Anwendung zurück, die die Anfrage gesendet hat.

Verwenden von Regeln in mehreren Regionen

Route 53 VPC Resolver ist ein regionaler Dienst, sodass Objekte, die Sie in einer AWS Region erstellen, nur in dieser Region verfügbar sind. Wenn Sie dieselbe Regel in mehr als einer Region verwenden möchten, müssen Sie die Regel in allen Regionen erstellen.

Das AWS Konto, das eine Regel erstellt hat, kann die Regel mit anderen AWS Konten gemeinsam nutzen. Weitere Informationen finden Sie unter Resolver-Regeln mit anderen AWS Konten teilen und gemeinsame Regeln verwenden.

Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstellt

Der Resolver erstellt automatisch definierte Systemregeln, die definieren, wie Abfragen für ausgewählte Domains standardmäßig aufgelöst werden:

- Für privat gehostete Zonen und für EC2 Amazon-spezifische Domainnamen (wie compute.amazonaws.com und compute.internal) stellen automatisch definierte Regeln sicher, dass Ihre privaten gehosteten Zonen und EC2 Instances weiterhin aufgelöst werden, wenn Sie bedingte Weiterleitungsregeln für weniger spezifische Domainnamen wie „“ erstellen. (Punkt) oder „com“.
- Für öffentlich reservierte Domainnamen (z. B. localhost und 10.in-addr.arpa) wird in den bewährten Methoden für DNS empfohlen, Abfragen lokal zu beantworten, anstatt sie an öffentliche Nameserver weiterzuleiten. Weitere Informationen finden Sie unter RFC 6303, Locally Served DNS Zones.

> **Note**
>
> Wenn Sie eine bedingte Weiterleitungsregel für "." (Punkt) oder "com" erstellen, empfehlen wir, auch eine Systemregel für amazonaws.com zu erstellen. (Systemregeln veranlassen VPC Resolver, DNS-Abfragen für bestimmte Domänen und Subdomänen lokal aufzulösen.) Die Erstellung dieser Systemregel verbessert die Leistung, reduziert die Anzahl der Anfragen, die an Ihr Netzwerk weitergeleitet werden, und senkt die VPC-Resolver-Gebühren.

Wenn Sie eine automatisch definierte Regel überschreiben möchten, können Sie eine bedingte Weiterleitungsregel für denselben Domainnamen erstellen.

Einige der automatisch definierten Regeln können auch deaktiviert werden. Weitere Informationen finden Sie unter Weiterleitungsregeln für Reverse-DNS-Abfragen in VPC Resolver.

VPC Resolver erstellt die folgenden automatisch definierten Regeln.

Regeln für privat gehostete Zonen

Für jede private gehostete Zone, die Sie einer VPC zuordnen, erstellt VPC Resolver eine Regel und ordnet sie der VPC zu. Wenn Sie die private gehostete Zone mehreren zuordnen VPCs, ordnet VPC Resolver die Regel derselben zu. VPCs

Die Regel verfügt über einen Typ von Forward (Weiterleiten).

Regeln für verschiedene AWS interne Domainnamen

Alle Regeln für die internen Domainnamen in diesem Abschnitt verfügen über einen Typ von Forward. VPC Resolver leitet DNS-Abfragen für diese Domainnamen an die autoritativen Nameserver für die VPC weiter.

> **Note**
>
> VPC Resolver erstellt die meisten dieser Regeln, wenn Sie das `enableDnsHostnames` Flag für eine VPC auf setzen. `true` VPC Resolver erstellt die Regeln auch dann, wenn Sie keine Resolver-Endpoints verwenden.

VPC Resolver erstellt die folgenden automatisch definierten Regeln und ordnet sie einer VPC zu, wenn Sie das `enableDnsHostnames` Flag für die VPC auf setzen: `true`

- *Region-name*.compute.internal, zum Beispiel eu-west-1.compute.internal. Die Region us-east-1 verwendet diesen Domainnamen nicht.
- *Region-name*.rechnen. *amazon-domain-name*, zum Beispiel eu-west-1.compute.amazonaws.com oder cn-north-1.compute.amazonaws.com.cn. Die Region us-east-1 verwendet diesen Domainnamen nicht.
- ec2.internal. Nur die Region us-east-1 verwendet diesen Domainnamen.
- compute-1.internal. Nur die Region us-east-1 verwendet diesen Domainnamen.
- compute-1.amazonaws.com. Nur die Region us-east-1 verwendet diesen Domänennamen.

Die folgenden automatisch definierten Regeln gelten für die umgekehrte DNS-Suche nach den Regeln, die VPC Resolver erstellt, wenn Sie das `enableDnsHostnames` Flag für die VPC auf setzen. `true`

- 10.in-addr.arpa
- 16.172.in-addr.arpa bis 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Regeln für jede der CIDR-Bereiche für die VPC. Wenn eine VPC beispielsweise einen CIDR-Bereich von 10.0.0.0/23 hat, erstellt VPC Resolver die folgenden Regeln:
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

Die folgenden automatisch definierten Regeln für localhost-bezogene Domains werden ebenfalls erstellt und mit einer VPC verknüpft, wenn für das Flag `enableDnsHostnames` `true` festgelegt wird:

- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa

VPC Resolver erstellt die folgenden automatisch definierten Regeln und ordnet sie Ihrer VPC zu, wenn Sie die VPC über Transit-Gateway oder VPC-Peering mit einer anderen VPC verbinden und die DNS-Unterstützung aktiviert ist:

- Die Reverse-DNS-Suche für die IP-Adressbereiche der Peer-VPC, z. B. 0.192.in-addr.arpa

Wenn Sie einer VPC einen IPv4 CIDR-Block hinzufügen, fügt VPC Resolver eine automatisch definierte Regel für den neuen IP-Adressbereich hinzu.

- Wenn sich die andere VPC in einer anderen Region befindet, die folgenden Domainnamen:
  - *Region-name*.compute.internal. Die Region us-east-1 verwendet diesen Domainnamen nicht.
  - *Region-name*. berechnen. *amazon-domain-name*. Die Region us-east-1 verwendet diesen Domainnamen nicht.
  - ec2.internal. Nur die Region us-east-1 verwendet diesen Domainnamen.
  - compute-1.amazonaws.com. Nur die Region us-east-1 verwendet diesen Domainnamen.

Eine Regel für alle anderen Domains

VPC Resolver erstellt ein „.“ (Punkt-) Regel, die für alle Domainnamen gilt, die nicht weiter oben in diesem Thema angegeben wurden. Die Regel „.“ hat den Typ Rekursiv, was bedeutet, dass die Regel bewirkt, dass VPC Resolver als rekursiver Resolver fungiert.

Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten

Bevor Sie Resolver-Endpoints für eingehenden und ausgehenden Datenverkehr in einer AWS Region erstellen, sollten Sie die folgenden Punkte berücksichtigen.

Themen

- Anzahl der eingehenden und ausgehenden Endpunkte in den einzelnen -Regionen
- Verwenden Sie dieselbe VPC für eingehende und ausgehende Endpunkte
- Eingehende Endpunkte und privat gehostete Zonen
- VPC-Peering
- IP-Adressen in freigegebenen Subnetzen
- Verbindung zwischen Ihrem Netzwerk und dem VPCs , in dem Sie Endpoints erstellen
- Wenn Sie Regeln freigeben, geben Sie auch ausgehende Endpunkte frei
- Auswählen von Protokollen für die Endpunkte
- Verwenden von VPC Resolver in VPCs , die für dedizierte Instance-Tenancy konfiguriert sind

Anzahl der eingehenden und ausgehenden Endpunkte in den einzelnen -Regionen

Wenn Sie DNS für eine AWS Region mit DNS für Ihr Netzwerk integrieren möchten, benötigen Sie VPCs in der Regel einen Resolver-Endpunkt für eingehende Anfragen (für DNS-Abfragen, die Sie an Ihren weiterleiten VPCs) und einen ausgehenden Endpunkt (für Anfragen, die Sie von Ihrem zu Ihrem Netzwerk weiterleiten). VPCs Sie können mehrere eingehende und mehrere ausgehende Endpunkte erstellen, aber ein eingehender oder ausgehender Endpunkt reicht aus, um die DNS-Abfragen für die jeweilige Richtung zu verarbeiten. Beachten Sie Folgendes:

- Für jeden Resolver-Endpunkt legen Sie zwei oder mehr IP-Adressen in verschiedenen Availability Zones fest. Jede IP-Adresse in einem Endpunkt kann eine große Anzahl von DNS-Abfragen pro Sekunde verarbeiten. (Informationen zu dem aktuellen Höchstwerten für die Anzahl der Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente auf Route 53 VPC Resolver.) Wenn Sie VPC Resolver benötigen, um mehr Abfragen zu verarbeiten, können Sie Ihrem vorhandenen Endpunkt mehr IP-Adressen hinzufügen, anstatt einen weiteren Endpunkt hinzuzufügen.
- Die Preise für VPC Resolver basieren auf der Anzahl der IP-Adressen in Ihren Endpunkten und auf der Anzahl der DNS-Abfragen, die der Endpunkt verarbeitet. Jeder Endpunkt enthält mindestens zwei IP-Adressen. Weitere Informationen zu den Preisen für VPC Resolver finden Sie unter Amazon Route 53-Preise.
- Jede Regel gibt den ausgehenden Endpunkt an, von dem DNS-Abfragen weitergeleitet werden. Wenn Sie mehrere ausgehende Endpunkte in einer AWS -Region erstellen und einige oder alle Resolver-Regeln mit einzelnen VPCs in Bezug setzen möchten, müssen Sie mehrere Kopien dieser Regeln erstellen.

Verwenden Sie dieselbe VPC für eingehende und ausgehende Endpunkte

Sie können eingehende und ausgehende Endpoints in derselben VPC oder in verschiedenen VPCs in derselben Region erstellen.

Weitere Informationen finden Sie unter Bewährte Methoden für Amazon Route 53.

Eingehende Endpunkte und privat gehostete Zonen

Wenn Sie möchten, dass VPC Resolver eingehende DNS-Abfragen mithilfe von Einträgen in einer privaten gehosteten Zone auflöst, ordnen Sie die private gehostete Zone der VPC zu, in der Sie den eingehenden Endpunkt erstellt haben. Informationen zum Zuordnen von privat gehosteten Zonen zu finden Sie unter. VPCs Arbeiten mit privat gehosteten Zonen

VPC-Peering

Sie können jede VPC in einer AWS Region für einen eingehenden oder ausgehenden Endpunkt verwenden, unabhängig davon, ob die von Ihnen gewählte VPC mit anderen gepeert wird. VPCs Weitere Informationen finden Sie unter Amazon Virtual Private Cloud VPC Peering.

IP-Adressen in freigegebenen Subnetzen

Wenn Sie einen eingehenden oder ausgehenden Endpunkt erstellen, können Sie nur dann eine IP-Adresse in einem freigegebenen Subnetz angeben, wenn das aktuelle Konto die VPC erstellt hat. Wenn ein anderes Konto eine VPC erstellt und ein Subnetz in der VPC für Ihr Konto freigibt, können Sie keine IP-Adresse in diesem Subnetz angeben. Weitere Informationen zu gemeinsam genutzten Subnetzen finden Sie unter Arbeiten mit geteilten Subnetzen VPCs im Amazon VPC-Benutzerhandbuch.

Verbindung zwischen Ihrem Netzwerk und dem VPCs , in dem Sie Endpoints erstellen

Sie benötigen eine der folgenden Verbindungen zwischen Ihrem Netzwerk und dem Netzwerk VPCs , in dem Sie Endgeräte erstellen:

- Eingehende Endpunkte - Sie müssen entweder eine Direct Connect-Verbindung oder eine VPN-Verbindung zwischen Ihrem Netzwerk und jeder VPC einrichten, für die Sie einen eingehenden Endpunkt erstellen.
- Ausgehende Endpunkte - Sie müssen eine Direct Connect-Verbindung, eine VPN-Verbindung oder ein Network Address Translation NAT-Gateway zwischen Ihrem Netzwerk und jeder VPC einrichten, für die Sie einen ausgehenden Endpunkt erstellen.

Wenn Sie Regeln freigeben, geben Sie auch ausgehende Endpunkte frei

Wenn Sie eine Regel erstellen, geben Sie den ausgehenden Endpunkt an, den VPC Resolver verwenden soll, um DNS-Abfragen an Ihr Netzwerk weiterzuleiten. Wenn Sie die Regel mit einem anderen AWS Konto teilen, teilen Sie indirekt auch den ausgehenden Endpunkt, den Sie in der Regel angeben. Wenn Sie für die Erstellung VPCs in einer AWS Region mehr als ein AWS Konto verwendet haben, können Sie wie folgt vorgehen:

- Einen ausgehenden Endpunkt in der Region erstellen.
- Erstellen Sie Regeln mit einem AWS Konto.
- Teilen Sie die Regeln mit allen AWS Konten, die VPCs in der Region erstellt wurden.

Auf diese Weise können Sie einen ausgehenden Endpunkt in einer Region verwenden, um DNS-Anfragen von mehreren an Ihr Netzwerk weiterzuleiten, VPCs auch wenn diese mit unterschiedlichen AWS Konten erstellt VPCs wurden.

Auswählen von Protokollen für die Endpunkte

Endpunktprotokolle bestimmen, wie Daten an einen eingehenden Endpunkt und von einem ausgehenden Endpunkt übertragen werden. Die Verschlüsselung von DNS-Abfragen für den VPC-Datenverkehr ist nicht erforderlich, da jeder Paketfluss im Netzwerk einzeln anhand einer Regel autorisiert wird, um die korrekte Quelle und das korrekte Ziel zu überprüfen, bevor er übertragen und zugestellt wird. Es ist höchst unwahrscheinlich, dass Informationen willkürlich zwischen Entitäten ausgetauscht werden, ohne dass dies von der sendenden und der empfangenden Entität ausdrücklich genehmigt wurde. Wenn ein Paket an ein Ziel geleitet wird, für das es keine passende Regel gibt, wird das Paket verworfen. Weitere Informationen finden Sie unter VPC-Features.

Die verfügbaren Protokolle sind:

- Do53: DNS über Port 53. Die Daten werden mithilfe des VPC Resolvers ohne zusätzliche Verschlüsselung weitergeleitet. Die Daten können zwar nicht von externen Parteien gelesen werden, können aber innerhalb der Netzwerke eingesehen werden. AWS Verwendet entweder UDP oder TCP, um die Pakete zu senden. Do53 wird hauptsächlich für den Verkehr innerhalb und zwischen Amazon VPCs verwendet. Derzeit ist dies das einzige Protokoll, das für die Delegierung eingehender Endpunkte verfügbar ist.
- DoH: Die Daten werden über eine verschlüsselte HTTPS-Sitzung übertragen. DoH fügt eine zusätzliche Sicherheitsstufe hinzu, bei der die Daten nicht von unbefugten Benutzern entschlüsselt werden können und von niemandem außer dem vorgesehenen Empfänger gelesen werden können. Nicht verfügbar für Delegierung eingehender Endpunkte.
- DoH-FIPS: Die Daten werden über eine verschlüsselte HTTPS-Sitzung übertragen, die mit dem Verschlüsselungsstandard FIPS 140-2 konform ist. Wird nur für eingehende Endpunkte unterstützt. Weitere Informationen finden Sie unter FIPS PUB 140-2. Nicht verfügbar für Delegierung eingehender Endpunkte.

Für einen eingehenden Endpunkt vom Typ Forward können Sie die Protokolle wie folgt anwenden:

- Do53 und DoH in Kombination.
- Do53 und DoH-FIPS in Kombination.
- Nur Do53.

- Nur DoH.
- Nur DoH-FIPS.
- Keins, was als Do53 behandelt wird.

Für einen ausgehenden Endpunkt können Sie die Protokolle wie folgt anwenden:

- Do53 und DoH in Kombination.
- Nur Do53.
- Nur DoH.
- Keins, was als Do53 behandelt wird.

Weitere Informationen finden Sie auch unter Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben und Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.

Verwenden von VPC Resolver in VPCs , die für dedizierte Instance-Tenancy konfiguriert sind

Wenn Sie einen Resolver-Endpunkt erstellen, können Sie keine VPC angeben, für die das Instance-Tenancy-Attribut auf `dedicated` festgelegt ist. VPC Resolver läuft nicht auf Single-Tenant-Hardware.

Sie können VPC Resolver weiterhin verwenden, um DNS-Abfragen aufzulösen, die ihren Ursprung in einer VPC haben. Erstellen Sie mindestens eine VPC, deren Instance-Tenancy-Attribut auf `default` festgelegt ist, und geben Sie diese VPC beim Erstellen von eingehenden und ausgehenden Endpunkten an.

Wenn Sie eine Weiterleitungsregel erstellen, können Sie diese mit einer beliebigen VPC verknüpfen, unabhängig von der Einstellung für das Instance-Tenancy-Attribut.

Verfügbarkeit und Skalierung von Route 53 VPC Resolver

Route 53 VPC Resolver, der auf der Amazon VPC CIDR + 2-Adresse und fd00:ec2: :253 ausgeführt wird, ist standardmäßig in allen verfügbar und reagiert rekursiv auf DNS-Abfragen für öffentliche Aufzeichnungen VPCs, Amazon VPC-spezifische DNS-Namen und Route 53-private gehostete Zonen. Der Route 53 VPC Resolver besteht aus zwei hochverfügbaren, für Benutzer transparenten

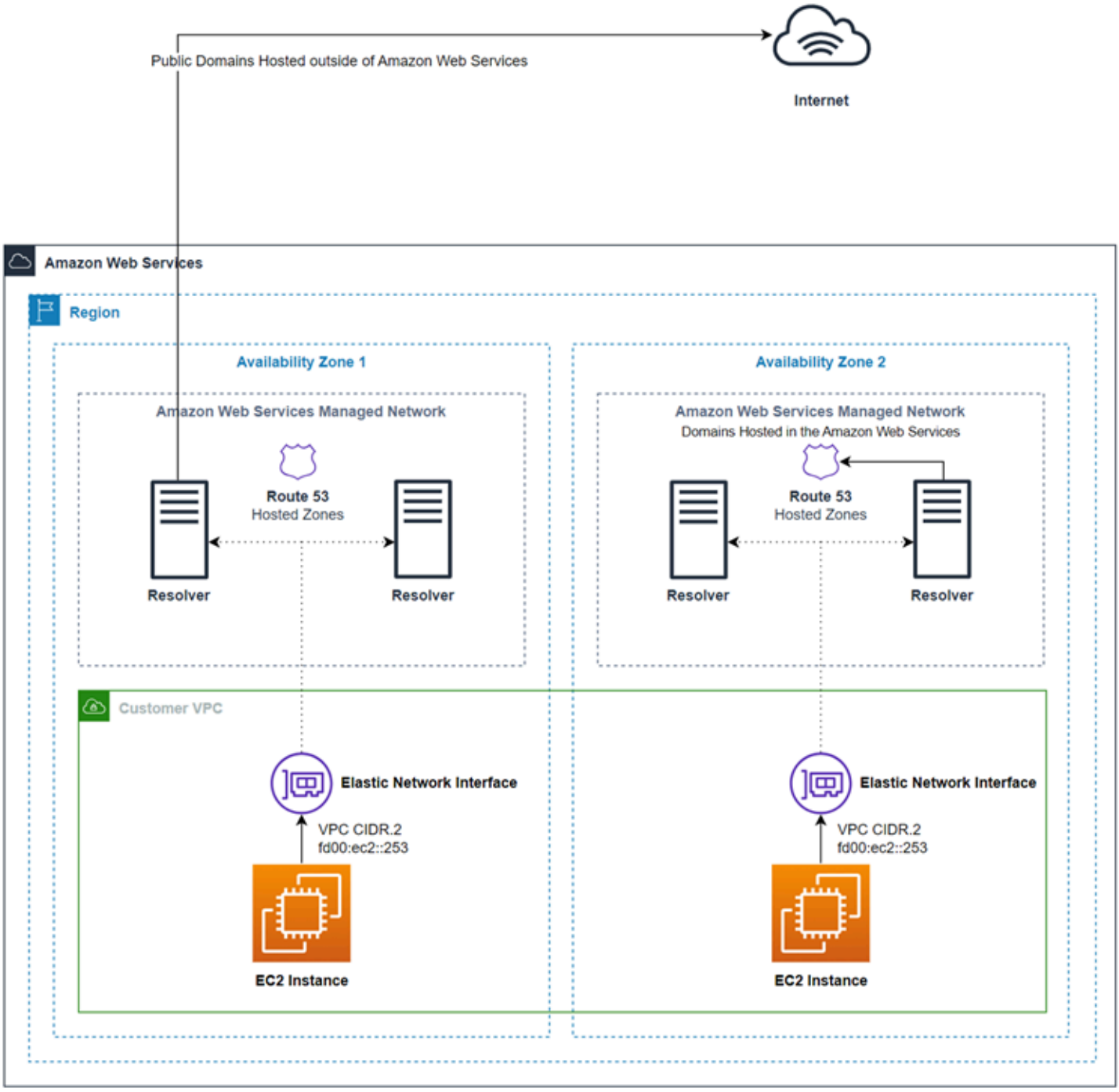
Komponenten: dem Nitro Resolver-Service und der Zonal Resolver-Flotte. Der Nitro Resolver Service ist ein Dienst, der auf Nitro-Instanzen auf der Nitro-Karte und in Instanzen der älteren Generation in Dom0 ausgeführt wird und Pakete, die an den Route 53 VPC Resolver adressiert sind, lokal auf dem Hostserver verarbeitet. Weitere Informationen finden Sie unter Das Sicherheitsdesign des Nitro-Systems. AWS

Der Nitro Resolver-Dienst verfügt über einen lokalen Cache, der dazu beitragen kann, die Latenz zu reduzieren, indem er auf wiederholte Anfragen reagiert, die über einen kurzen Zeitraum von einer Instanz gestellt werden. Wenn der Nitro Resolver-Dienst eine Anfrage empfängt, für die er keine zwischengespeicherte Antwort hat, leitet er die Anfrage an die Zonal Resolver-Flotte weiter, eine hochverfügbare Flotte von Resolvern, die sich normalerweise in derselben Availability Zone wie die Instance befindet. Wenn bei der Verarbeitung von Abfragen durch Upstream-Nameserver oder andere Komponenten im Pfad Fehler auftreten, ist der Nitro Resolver-Dienst häufig in der Lage, diese Fehler transparent zu behandeln, ohne dass sich dies auf die Workloads auswirkt, die auf der Instanz ausgeführt werden. Wenn der Resolver außerdem auf Abfrage-Timeouts, abgelehnte Verbindungen oder SERVFAILS von den Nameservern der Domain stößt, kann er mit einer zwischengespeicherten Antwort antworten, die über dem (TTL) -Wert liegt, um die Time-To-Live Verfügbarkeit zu verbessern. Abfragen zwischen dem Nitro Resolver-Service und der Zonal Resolver-Flotte sind auf ein streng kontrolliertes Netzwerk außerhalb der Kunden-VPC beschränkt, das für Kunden nicht zugänglich ist und strengen Sicherheitskontrollen unterliegt. Durch die Bearbeitung von Anfragen zwischen dem Nitro Resolver-Service und der Zonal Resolver-Flotte außerhalb der VPC werden Kunden daran gehindert, DNS-Abfragen innerhalb ihrer VPC abzufangen. Anfragen, die an Nameserver außerhalb von gerichtet sind, durchqueren das öffentliche Internet und stammen von AWS öffentlichen IP-Adressen, die zur Zonal Resolver-Flotte gehören. Das Subnetzattribut eDNS0-Client wird derzeit nicht unterstützt, was bedeutet, dass alle Anfragen, die an öffentliche DNS-Nameserver gerichtet sind, keine Informationen über die ursprüngliche Kunden-IP-Adresse enthalten.

Der Nitro Resolver-Dienst ist Teil der Link-Local-Dienste auf der Instanz. Zu den Link-Local-Services gehören Route 53 VPC Resolver, Amazon Time Service (NTP), Instance Metadata Service (IMDS) und Windows Licensing Service (für Windows-Instances). Diese Dienste skalieren mit jeder elastic network interface, die Sie in Ihrer VPC erstellen, und jede Netzwerkschnittstelle erlaubt 1024 Pakete pro Sekunde (PPS), die für Link-Local-Services bestimmt sind. Pakete, die dieses Limit überschreiten, werden zurückgewiesen. Anhand des von ethtool zurückgegebenen `linklocal_allowance_exceeded` Werts können Sie feststellen, ob Sie dieses Limit überschritten haben. Weitere Informationen zum Ethtool finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2 Amazon-Instance im EC2 Amazon-Benutzerhandbuch. Diese Metrik kann vom CloudWatch Agenten auch an CloudWatch Metriken gemeldet werden. Da der Route 53 VPC Resolver pro

Netzwerkschnittstelle implementiert wird, skaliert er und wird zuverlässiger, je mehr Instances in mehr Availability Zones hinzugefügt werden. Es gibt kein aggregiertes Limit pro VPC für die Anzahl der Abfragen, sodass der Route 53 VPC Resolver innerhalb der Grenzen einer VPC skalieren kann, die inhärent auf der Netzwerkadressnutzung (NAU) basiert. Weitere Informationen finden Sie unter Verwendung der Netzwerkadresse für Ihre VPC im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Das folgende Diagramm zeigt einen Überblick darüber, wie Route 53 VPC Resolver DNS-Abfragen innerhalb von Availability Zones auflöst.



Erste Schritte mit Route 53 VPC Resolver

Die Route 53 VPC Resolver-Konsole enthält einen Assistenten, der Sie durch die folgenden Schritte für die ersten Schritte mit VPC Resolver führt:

- Endpunkte erstellen: eingehend, ausgehend oder beides.

- Erstellen Sie für ausgehende Endpunkte eine oder mehrere Weiterleitungsregeln, die die Domainnamen angeben, für die Sie DNS-Abfragen an Ihr Netzwerk weiterleiten möchten.
- Wenn Sie einen ausgehenden Endpunkt erstellt haben, wählen Sie die VPC aus, mit der Sie die Regeln verknüpfen möchten.

So konfigurieren Sie Route 53 VPC Resolver mit dem Assistenten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die VPC Resolver-Konsole unter. https://console.aws.amazon.com/route53resolver/
2. Wählen Sie auf der Seite Willkommen bei Route 53 VPC Resolver die Option Endpoints konfigurieren aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie einen Resolver-Endpunkt erstellen möchten.
4. Wählen Sie unter Basic configuration (Grundlegende Konfiguration), in welche Richtung DNS-Abfragen weitergeleitet werden sollen:

   - Eingehend und ausgehend: Der Assistent führt Sie durch die Einstellungen, mit denen Sie sowohl DNS-Anfragen von Resolvern in Ihrem Netzwerk an den VPC-Resolver in einer VPC weiterleiten als auch bestimmte Abfragen (wie example.com oder example.net) von einer VPC an Resolver in Ihrem Netzwerk weiterleiten können.
   - Nur eingehend: Der Assistent führt Sie durch die Einstellungen, mit denen Sie DNS-Abfragen von Resolvern in Ihrem Netzwerk an den VPC-Resolver in einer VPC weiterleiten können.
   - Outbound only (Nur ausgehend): Der Assistent führt Sie durch die Einstellungen, mit denen Sie bestimmte Abfragen von einer VPC an Resolver in Ihrem Netzwerk weiterleiten können.
5. Wählen Sie Weiter aus.
6. Wenn Sie Inbound and outbound (Eingehend und ausgehend) oder Inbound only (Nur eingehend) ausgewählt haben, geben Sie die entsprechenden Werte für die Konfiguration eines eingehenden Endpunkts an. Fahren Sie danach mit Schritt 7 fort. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben.

   Wenn Sie Outbound only (Nur ausgehend) ausgewählt haben, fahren Sie mit Schritt 7 fort.
7. Geben Sie die entsprechenden Werte für die Konfiguration eines ausgehenden Endpunkts an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.

8. Wenn Sie Inbound and outbound (Eingehend und ausgehend) oder Outbound only (Nur ausgehend) ausgewählt haben, geben Sie die entsprechenden Werte für die Erstellung einer Regel an. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.
9. Vergewissern Sie sich auf der Seite Review and create (Überprüfen und erstellen), dass die Einstellungen, die Sie auf den vorherigen Seiten angegeben haben, korrekt sind. Wählen Sie ggf. Edit (Bearbeiten) für den entsprechenden Abschnitt aus und aktualisieren Sie die Einstellungen. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf Submit (Absenden).

   > **Note**
   >
   > Die Erstellung eines ausgehenden Endpunkt nimmt ein oder zwei Minuten in Anspruch. Sie können erst einen anderen ausgehenden Endpunkt erstellen, wenn der erste erstellt wurde.

10. Wenn Sie weitere Regeln erstellen möchten, informieren Sie sich unter Verwalten von Weiterleitungsregeln.
11. Wenn Sie einen eingehenden Endpunkt erstellt haben, konfigurieren Sie DNS-Resolver in Ihrem Netzwerk so, dass die entsprechenden DNS-Abfragen an die IP-Adressen für Ihren eingehenden Endpunkt weitergeleitet werden. Weitere Informationen finden Sie in der Dokumentation zu Ihrer DNS-Anwendung.

Weiterleiten eingehender DNS-Anfragen an Ihren VPCs

Um DNS-Anfragen von Ihrem Netzwerk an VPC Resolver weiterzuleiten, erstellen Sie einen eingehenden Endpunkt. Ein eingehender Endpunkt gibt die IP-Adressen (aus dem Bereich der für Ihre VPC verfügbaren IP-Adressen) an, an die DNS-Resolver im Netzwerk DNS-Abfragen weiterleiten sollen. Diese IP-Adressen sind keine öffentlichen IP-Adressen. Daher müssen Sie für jeden eingehenden Endpunkt Ihre VPC entweder über eine Direct Connect Verbindung oder eine VPN-Verbindung mit Ihrem Netzwerk verbinden.

Bei der Implementierung eingehender Delegierung delegieren Sie die DNS-Autorität für eine Subdomain von Ihrer lokalen DNS-Infrastruktur an VPC Resolver. Um diese Delegierung ordnungsgemäß zu konfigurieren, müssen Sie die IP-Adressen des eingehenden Endpunkts als Glue-Records (NS-Einträge) auf Ihrem lokalen Nameserver für die Subdomain verwenden, die delegiert wird. Wenn Sie beispielsweise die Subdomain „aws.example.com“ über einen eingehenden Delegierungsendpunkt mit den IP-Adressen 10.0.1.100 und 10.0.1.101 an VPC Resolver delegieren,

würden Sie auf Ihrem lokalen DNS-Server NS-Einträge erstellen, die „aws.example.com“ auf diese IP-Adressen verweisen. Dadurch wird sichergestellt, dass DNS-Abfragen für die delegierte Subdomain ordnungsgemäß über den Eingangsendpunkt an den VPC-Resolver weitergeleitet werden, sodass der VPC-Resolver mit Datensätzen aus der zugehörigen privaten Hosting-Zone antworten kann.

Konfigurieren von Weiterleitungen eingehender Abfragen

Gehen Sie wie folgt vor, um einen eingehenden Endpunkt zu erstellen.

So erstellen Sie einen eingehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Inbound endpoints (Eingehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie einen eingehenden Endpunkt erstellen möchten.
4. Klicken Sie auf Create inbound endpoint (Eingehenden Endpunkt erstellen).
5. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben.
6. Wählen Sie Erstellen aus.
7. Konfigurieren Sie DNS-Resolver in Ihrem Netzwerk so, dass die entsprechenden DNS-Abfragen an die IP-Adressen für Ihren eingehenden Endpunkt weitergeleitet werden. Weitere Informationen finden Sie in der Dokumentation zu Ihrer DNS-Anwendung.

Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben

Wenn Sie einen eingehenden Endpunkt erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Außenposten-ID

Wenn Sie den Endpunkt für einen VPC-Resolver auf einer AWS Outposts VPC erstellen, ist dies die ID. AWS Outposts

Endpoint name (Endpunktname)

Ein Anzeigename, mit dem Sie ganz einfach einen eingehenden Endpunkt auf dem Dashboard finden können.

Endpunktkategorie

Wählen Sie entweder Standard oder Delegierung. Wenn die Kategorie Standard ist, leitet der Resolver in Ihrem Netzwerk die DNS-Anfragen an die IP-Adresse des eingehenden Endpunkts weiter. Wenn die Kategorie Delegierung lautet, wird die Autorität für eine Domain an den VPC Resolver delegiert.

VPC in der Region region-name

Alle eingehenden DNS-Anfragen aus Ihrem Netzwerk passieren diese VPC auf dem Weg zum VPC Resolver.

Sicherheitsgruppe für diesen Endpunkt

Die ID einer oder mehrerer Sicherheitsgruppen, die Sie verwenden möchten, um den Zugriff auf diese VPC zu steuern. Die von Ihnen angegebene Sicherheitsgruppe muss eine oder mehrere eingehende Regeln enthalten. Eingehende Regeln müssen TCP- und UDP-Zugriff auf Port 53 zulassen. Wenn Sie das DoH-Protokoll verwenden, müssen Sie auch Port 443 in der Sicherheitsgruppe zulassen. Sie können diesen Wert nicht ändern, nachdem Sie den Endpunkt erstellt haben.

Einige Sicherheitsgruppenregeln sorgen dafür, dass Ihre Verbindung nachverfolgt wird, und die maximale Gesamtzahl der Abfragen pro Sekunde pro IP-Adresse für einen eingehenden Endpunkt kann bis zu 1500 betragen. Informationen zur Vermeidung der durch eine Sicherheitsgruppe verursachten Verbindungsverfolgung finden Sie unter Verbindungen ohne Nachverfolgung.

> **Note**
>
> Verwenden Sie den AWS CLI Befehl`create-resolver-endpoint`, um mehrere Sicherheitsgruppen hinzuzufügen. Weitere Informationen finden Sie unter create-resolver-endpoint.

Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Endpunkttyp

Der Endpunkttyp kann entweder IPv4 IPv6, oder Dual-Stack-IP-Adressen sein. Bei einem Dual-Stack-Endpunkt hat der Endpunkt IPv4 sowohl eine Adresse als auch eine IPv6 Adresse, an die Ihr DNS-Resolver in Ihrem Netzwerk DNS-Anfragen weiterleiten kann.

> **Note**
>
> Aus Sicherheitsgründen verweigern wir allen Dual-Stack- und IP-Adressen den direkten IPv6 Datenzugriff aus dem öffentlichen Internet. IPv6

IP-Adressen

Die IP-Adressen, an die DNS-Resolver in Ihrem Netzwerk DNS-Abfragen weiterleiten sollen. Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben. Wenn Sie einen eingehenden Delegationsendpunkt erstellt haben, verwenden Sie diese IP-Adressen als Glue-NS-Einträge für die Subdomain, für die Sie die Autorität an VPC Resolver delegieren möchten. Beachten Sie Folgendes:

Mehrere Availability Zones

Wir empfehlen, IP-Adressen in mindestens zwei Availability Zones festzulegen. Wahlweise können Sie zusätzliche IP-Adressen in diesen oder anderen Availability Zones angeben.

IP-Adressen und Amazon VPC Elastic Network-Schnittstellen

Für jede Kombination aus Availability Zone, Subnetz und IP-Adresse, die Sie angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente auf Route 53 VPC Resolver. Weitere Informationen zu den Preisen für die einzelnen Elastic Network-Schnittstellen finden Sie unter "Amazon Route 53" auf der Seite Amazon Route 53 Preise.

> **Note**
>
> Der Resolver-Endpunkt hat eine private IP-Adresse. Diese IP-Adressen ändern sich im Laufe der Lebensdauer eines Endpunkts nicht.

Geben Sie für jede IP-Adresse die folgenden Werte an. Jede IP-Adresse muss in einer Availability Zone in der VPC vorhanden sein, die Sie in VPC in der Region region-name angegeben haben.

Availability Zone

Die Availability Zone, die DNS-Abfragen auf dem Weg zu Ihrer VPC durchlaufen sollen. Die angegebene Availability Zone muss mit einem Subnetz konfiguriert sein.

Subnetz

Das Subnetz, das die IP-Adressen enthält, die Sie Ihrem Resolver-Endpunkt zuweisen möchten. ENIs Dies sind die Adressen, an die Sie DNS-Anfragen senden werden. Das Subnetz muss eine verfügbare IP-Adresse enthalten.

Die Subnetz-IP-Adresse muss dem Endpunkttyp entsprechen.

IP-Adresse

Die IP-Adresse, die Sie den eingehenden Endpunkten zuweisen möchten.

Wählen Sie aus, ob VPC Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst angeben möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie entweder eine IPv6 Oder-Adresse IPv4 oder beide ein.

Protokolle

Das Endpunktprotokoll bestimmt, wie die Daten an den eingehenden Endpunkt übertragen werden. Wählen Sie ein oder mehrere Protokolle, je nachdem, welche Sicherheitsstufe Sie benötigen.

- Do53: (Standard) Die Daten werden mit dem Route 53 VPC Resolver ohne zusätzliche Verschlüsselung weitergeleitet. Die Daten können zwar nicht von externen Parteien gelesen werden, können aber innerhalb der Netzwerke eingesehen werden. AWS Dies ist das einzige Protokoll, das derzeit für die Kategorie eingehende Delegationsendpunkte verfügbar ist.
- DoH: Die Daten werden über eine verschlüsselte HTTPS-Sitzung übertragen. DoH fügt eine zusätzliche Sicherheitsstufe hinzu, bei der die Daten nicht von unbefugten Benutzern entschlüsselt werden können und von niemandem außer dem vorgesehenen Empfänger gelesen werden können.

- DoH-FIPS: Die Daten werden über eine verschlüsselte HTTPS-Sitzung übertragen, die mit dem Verschlüsselungsstandard FIPS 140-2 konform ist. Wird nur für eingehende Endpunkte unterstützt. Weitere Informationen finden Sie unter FIPS PUB 140-2.

> **Note**
>
> Bei eingehenden DOH/DOH-FIPS-Endpunkten ist ein Problem bekannt, bei dem eine falsche Quell-IP in der VPC Resolver-Abfrageprotokollierung veröffentlicht wird.

Für einen eingehenden Endpunkt können Sie die Protokolle wie folgt anwenden:

- Do53 und DoH in Kombination.
- Do53 und DoH-FIPS in Kombination.
- Nur Do53.
- Nur DoH.
- Nur DoH-FIPS.
- Keins, was als Do53 behandelt wird.

> **Important**
>
> Sie können das Protokoll eines eingehenden Endpunkts nicht direkt von nur Do53 auf nur DoH oder DoH-FIPS ändern. Damit soll eine plötzliche Unterbrechung des eingehenden Datenverkehrs verhindert werden, der auf Do53 angewiesen ist. Um das Protokoll von Do53 auf DoH oder DoH-FIPS zu ändern, müssen Sie zunächst sowohl Do53 als auch DoH oder Do53 und DoH-FIPS aktivieren, um sicherzustellen, dass der gesamte eingehende Datenverkehr auf das DoH-Protokoll oder DoH-FIPS umgestellt wurde, und dann Do53 entfernen.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Verwalten von eingehenden Endpunkten

Um eingehende Endpunkte zu verwalten, führen Sie die entsprechenden Schritte aus.

Themen

Anzeigen und Bearbeiten von eingehenden Endpunkten

Führen Sie zum Anzeigen und Bearbeiten von Einstellungen für einen eingehenden Endpunkt die folgenden Schritte aus.

Anzeigen und Bearbeiten von Einstellungen für einen eingehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Inbound endpoints (Eingehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den eingehenden Endpunkt erstellt haben.
4. Wählen Sie die Option für den Endpunkt, für den Sie Einstellungen anzeigen oder den Sie bearbeiten möchten.
5. Wählen Sie View details (Details anzeigen) oder Edit (Bearbeiten).

   Informationen zu den Werten für eingehende Endpunkte finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben.
6. Wenn Sie Edit (Bearbeiten) gewählt haben, geben Sie die entsprechenden Werte ein und klicken Sie anschließend auf Save (Speichern).

Anzeigen des Status für eingehende Endpunkte

Gehen Sie folgendermaßen vor, um den Status eines eingehenden Endpunkts anzuzeigen.

So zeigen Sie den Status eines eingehenden Endpunkts an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Inbound endpoints (Eingehende Endpunkte).

3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den eingehenden Endpunkt erstellt haben. Die Spalte Status enthält einen der folgenden Werte:

   Erstellen

   VPC Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

   Betriebsbereit

   Die Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt sind korrekt konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und VPC Resolver weiterleiten.

   Aktualisieren

   VPC Resolver verknüpft oder trennt eine oder mehrere Netzwerkschnittstellen mit diesem Endpunkt.

   Automatische Wiederherstellung

   VPC Resolver versucht, eine oder mehrere der Netzwerkschnittstellen wiederherzustellen, die diesem Endpunkt zugeordnet sind. Während der Wiederherstellung funktioniert der Endpunkt aufgrund des Limits für die Anzahl der DNS-Abfragen pro IP-Adresse (pro Netzwerkschnittstelle) mit begrenzter Kapazität. Das aktuelle Limit finden Sie unter Kontingente auf Route 53 VPC Resolver.

   Aktion erforderlich

   Dieser Endpunkt ist fehlerhaft und VPC Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zugeordnet haben. Fügen Sie für jede IP-Adresse, die nicht verfügbar ist, eine andere IP-Adresse hinzu und löschen Sie dann die nicht verfügbare IP-Adresse. (Ein Endpunkt muss immer mindestens zwei IP-Adressen enthalten.) Ein Status von Aktion erforderlich kann verschiedene Ursachen haben. Hier sind zwei häufige Ursachen:

   - Eine oder mehrere Netzwerkschnittstellen, die diesem Endpunkt zugeordnet sind, wurden mit Amazon VPC gelöscht.
   - Die Netzwerkschnittstelle konnte aus einem Grund nicht erstellt werden, der nicht der Kontrolle von VPC Resolver unterliegt.

Löschen

VPC Resolver löscht diesen Endpunkt und die zugehörigen Netzwerkschnittstellen.

Löschen von eingehenden Endpunkten

Gehen Sie wie folgt vor, um einen eingehenden Endpunkt zu löschen.

> **Important**
>
> Wenn Sie einen eingehenden Endpunkt löschen, werden DNS-Anfragen aus Ihrem Netzwerk nicht mehr an den VPC Resolver in der VPC weitergeleitet, die Sie im Endpunkt angegeben haben.

So löschen Sie einen eingehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Inbound endpoints (Eingehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den eingehenden Endpunkt erstellt haben.
4. Wählen Sie die Option für den Endpunkt, den Sie löschen möchten.
5. Wählen Sie Löschen aus.
6. Um zu bestätigen, dass Sie den Endpunkt löschen möchten, geben Sie den Namen des Endpunkts ein und wählen Sie Submit (Senden).

Weiterleiten von ausgehenden DNS-Abfragen an Ihr Netzwerk

Um DNS-Anfragen, die von EC2 Amazon-Instances in einer oder mehreren Instanzen stammen, VPCs an Ihr Netzwerk weiterzuleiten, erstellen Sie einen ausgehenden Endpunkt und eine oder mehrere Regeln:

Ausgehender Endpunkt

Um DNS-Anfragen von Ihrem VPCs an Ihr Netzwerk weiterzuleiten, erstellen Sie einen ausgehenden Endpunkt. Ein ausgehender Endpunkt gibt die IP-Adressen an, von denen Abfragen

stammen. Diese aus dem Bereich der IP-Adressen ausgewählten IP-Adressen, die Ihrer VPC zur Verfügung stehen, sind keine öffentlichen IP-Adressen. Dies bedeutet, dass Sie für jeden ausgehenden Endpunkt Ihre VPC über eine Direct Connect VPC-Verbindung oder ein NAT-Gateway (Network Address Translation) mit Ihrem Netzwerk verbinden müssen. Beachten Sie, dass Sie denselben ausgehenden Endpunkt für mehrere Endpunkte VPCs in derselben Region verwenden oder mehrere ausgehende Endpunkte erstellen können. Wenn Sie möchten, dass Ihr ausgehender Endpunkt verwendet wird DNS64, können Sie die DNS64 Verwendung von Amazon Virtual Private Cloud aktivieren. Weitere Informationen finden Sie unter DNS64 und NAT64 im Amazon VPC-Benutzerhandbuch.

Die Ziel-IP aus der VPC-Resolver-Regel wird vom VPC Resolver nach dem Zufallsprinzip ausgewählt, und die Auswahl einer bestimmten Ziel-IP gegenüber der anderen wird nicht bevorzugt. Wenn eine Ziel-IP nicht auf die weitergeleitete DNS-Anfrage reagiert, versucht der VPC-Resolver erneut, eine zufällige IP-Adresse unter den Zielen auszuwählen. IPs

Stellen Sie sicher, dass alle Ziel-IP-Adressen von den Resolver-Endpunkten aus erreichbar sind. Wenn VPC Resolver ausgehende DNS-Anfragen nicht an eine der Ziel-IP-Adressen weiterleiten kann, kann dies zu längeren DNS-Auflösungszeiten führen.

Regeln

Sie erstellen eine oder mehrere Regeln, um die Domainnamen der Abfragen anzugeben, die Sie an die DNS-Resolver in Ihrem Netzwerk weiterleiten möchten. Jede Weiterleitungsregel spezifiziert einen Domainnamen. Anschließend ordnen Sie den Personen, VPCs für die Sie Abfragen an Ihr Netzwerk weiterleiten möchten, Regeln zu.

Die Regeln für die Delegierung ausgehender Nachrichten folgen bestimmten Delegierungsprinzipien, die sich von den Standardweiterleitungsregeln unterscheiden. Wenn Sie eine Delegierungsregel erstellen, vergleicht VPC Resolver die Delegierungsdatensätze in der Regel mit den NS-Einträgen in DNS-Antworten, um festzustellen, ob eine Delegierung erfolgen soll. Der VPC-Resolver delegiert die Autorität nur dann an Ihre lokalen Resolver, wenn eine Übereinstimmung zwischen der Konfiguration der Delegierungsregeln und den tatsächlichen NS-Einträgen besteht, die in der DNS-Antwort zurückgegeben wurden. Im Gegensatz zu Weiterleitungsregeln, die Anfragen auf der Grundlage des Abgleichs von Domainnamen umleiten, respektieren Delegierungsregeln die DNS-Delegierungskette und werden nur aktiviert, wenn die autoritativen Nameserver in der Antwort mit der Delegierungskonfiguration übereinstimmen.

Weitere Informationen finden Sie unter den folgenden Themen:

- Private hosted zones that have overlapping namespaces

- Private hosted zones and Route 53 VPC Resolver rules

Konfigurieren von Weiterleitungen ausgehender Abfragen

Gehen Sie wie folgt vor, um VPC Resolver so zu konfigurieren, dass DNS-Abfragen, die von Ihrer VPC stammen, an Ihr Netzwerk weitergeleitet werden.

> **Important**
>
> Nachdem Sie einen ausgehenden Endpunkt erstellt haben, müssen Sie eine oder mehrere Regeln erstellen und diese einer oder mehreren Regeln zuordnen. VPCs Regeln geben die Domainnamen der DNS-Abfragen an, die Sie an Ihr Netzwerk weiterleiten möchten.

So erstellen Sie einen ausgehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Outbound endpoints (Ausgehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie einen ausgehenden Endpunkt erstellen möchten.
4. Klicken Sie auf Create outbound endpoint (Ausgehenden Endpunkt erstellen).
5. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.
6. Wählen Sie Erstellen aus.

   > **Note**
   >
   > Die Erstellung eines ausgehenden Endpunkt nimmt ein oder zwei Minuten in Anspruch. Sie können erst einen anderen ausgehenden Endpunkt erstellen, wenn der erste erstellt wurde.

7. Erstellen Sie eine oder mehrere Regeln, um die Domainnamen der DNS-Abfragen anzugeben, die Sie an Ihr Netzwerk weiterleiten möchten. Weitere Informationen finden Sie im nächsten Verfahren .

Führen Sie die folgenden Schritte aus, um eine oder mehrere Weiterleitungsregeln zu erstellen.

Um Weiterleitungsregeln zu erstellen und die Regeln einer oder mehreren zuzuordnen VPCs

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie Regel erstellen aus.
5. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.
6. Wählen Sie Save (Speichern) aus.
7. Um eine weitere Regel hinzuzufügen, wiederholen Sie die Schritte 4 bis 6.

Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben

Wenn Sie einen ausgehenden Endpunkt erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Außenposten-ID

Wenn Sie den Endpunkt für einen VPC-Resolver auf einer AWS Outposts VPC erstellen, ist dies die ID. AWS Outposts

Endpoint name (Endpunktname)

Ein Anzeigename, mit dem Sie ganz einfach einen ausgehenden Endpunkt auf dem Dashboard finden können.

VPC in der Region region-name

Alle ausgehenden DNS-Abfragen durchlaufen diese VPC auf dem Weg zu Ihrem Netzwerk.

Sicherheitsgruppe für diesen Endpunkt

Die ID einer oder mehrerer Sicherheitsgruppen, die Sie verwenden möchten, um den Zugriff auf diese VPC zu steuern. Die von Ihnen angegebene Sicherheitsgruppe muss eine oder mehrere ausgehende Regeln enthalten. Ausgehende Regeln müssen TCP- und UDP-Zugriff auf dem Port

zulassen, den Sie für DNS-Abfragen in Ihrem Netzwerk verwenden. Sie können diesen Wert nicht ändern, nachdem Sie ein Portal erstellt haben.

Einige Sicherheitsgruppenregeln sorgen dafür, dass Ihre Verbindung nachverfolgt wird, und wirken sich möglicherweise auf die maximale Anzahl von Abfragen pro Sekunde vom ausgehenden Endpunkt zum Ziel-Nameserver aus. Informationen zur Vermeidung der durch eine Sicherheitsgruppe verursachten Verbindungsverfolgung finden Sie unter Verbindungen ohne Nachverfolgung.

Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Endpunkttyp

Der Endpunkttyp kann entweder IPv4 IPv6, oder Dual-Stack-IP-Adressen sein. Bei einem Dual-Stack-Endpunkt hat der Endpunkt IPv4 sowohl eine Adresse als auch eine IPv6 Adresse, an die Ihr DNS-Resolver in Ihrem Netzwerk DNS-Anfragen weiterleiten kann.

> **Note**
>
> Aus Sicherheitsgründen verweigern wir allen Dual-Stack- und IP-Adressen den direkten IPv6 Datenzugriff auf das öffentliche Internet. IPv6

IP-Adressen

Die IP-Adressen in Ihrer VPC, an die VPC Resolver DNS-Abfragen auf dem Weg zu Resolvern in Ihrem Netzwerk weiterleiten soll. Dies sind nicht die IP-Adressen der DNS-Resolver in Ihrem Netzwerk. Sie geben die Resolver-IP-Adressen an, wenn Sie die Regeln erstellen, die Sie einem oder mehreren zuordnen. VPCs Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben.

> **Note**
>
> Der Resolver-Endpunkt hat eine private IP-Adresse. Diese IP-Adressen ändern sich im Laufe der Lebensdauer eines Endpunkts nicht.

Beachten Sie Folgendes:

Mehrere Availability Zones

Wir empfehlen, IP-Adressen in mindestens zwei Availability Zones festzulegen. Wahlweise können Sie zusätzliche IP-Adressen in diesen oder anderen Availability Zones angeben.

IP-Adressen und Amazon VPC Elastic Network-Schnittstellen

Für jede Kombination aus Availability Zone, Subnetz und IP-Adresse, die Sie angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente auf Route 53 VPC Resolver. Weitere Informationen zu den Preisen für die einzelnen Elastic Network-Schnittstellen finden Sie unter "Amazon Route 53" auf der Seite Amazon Route 53 Preise.

Reihenfolge der IP-Adressen

Sie können IP-Adressen in beliebiger Reihenfolge angeben. Bei der Weiterleitung von DNS-Abfragen wählt VPC Resolver IP-Adressen nicht anhand der Reihenfolge aus, in der die IP-Adressen aufgeführt sind.

Geben Sie für jede IP-Adresse die folgenden Werte an. Jede IP-Adresse muss in einer Availability Zone in der VPC vorhanden sein, die Sie in VPC in der Region region-name angegeben haben.

Availability Zone

Die Availability Zone, die DNS-Abfragen auf dem Weg zu Ihrem Netzwerk durchlaufen sollen. Die angegebene Availability Zone muss mit einem Subnetz konfiguriert sein.

Subnetz

Das Subnetz mit der IP-Adresse, aus denen die DNS-Abfragen auf dem Weg zu Ihrem Netzwerk stammen sollen. Das Subnetz muss eine verfügbare IP-Adresse enthalten.

Die Subnetz-IP-Adresse muss dem Endpunkttyp entsprechen.

IP-Adresse

Die IP-Adresse, von der die DNS-Abfragen auf dem Weg zu Ihrem Netzwerk stammen sollen.

Wählen Sie aus, ob VPC Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst angeben möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie eine IPv6 Oder-Adresse IPv4 oder beide ein.

Protokolle

Das Endpunktprotokoll bestimmt, wie die Daten vom ausgehenden Endpunkt übertragen werden. Wählen Sie ein oder mehrere Protokolle, je nachdem, welche Sicherheitsstufe Sie benötigen.

- Do53: (Standard) Die Daten werden mit dem Route 53 VPC Resolver ohne zusätzliche Verschlüsselung weitergeleitet. Die Daten können zwar nicht von externen Parteien gelesen werden, aber sie können innerhalb der AWS -Netzwerke eingesehen werden.
- DoH: Die Daten werden über eine verschlüsselte HTTPS-Sitzung übertragen. DoH fügt eine zusätzliche Sicherheitsstufe hinzu, bei der die Daten nicht von unbefugten Benutzern entschlüsselt werden können und von niemandem außer dem vorgesehenen Empfänger gelesen werden können.

Für einen ausgehenden Endpunkt können Sie die Protokolle wie folgt anwenden:

- Do53 und DoH in Kombination.
- Nur Do53.
- Nur DoH.
- Keins, was als Do53 behandelt wird.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben

Wenn Sie eine Weiterleitungsregel erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Regelname

Ein Anzeigename, mit dem Sie ganz einfach eine Regel auf dem Dashboard finden können.

Art der Regel

Wählen Sie einen geeignete Wert aus:

- Forward (Weiterleiten) – Wählen Sie diese Option, wenn Sie DNS-Abfragen für einen angegebenen Domainnamen an Resolver in Ihrem Netzwerk weiterleiten möchten.
- Delegieren — Wählen Sie diese Option, wenn Sie die Autorität für eine Subdomain, die in einer privaten Hosting-Zone gehostet wird, an Ihren lokalen Resolver (oder an einen VPC-Resolver auf einer anderen VPC) delegieren möchten.

- System — Wählen Sie diese Option, wenn Sie möchten, dass VPC Resolver das in einer Weiterleitungsregel definierte Verhalten selektiv überschreibt. Wenn Sie eine Systemregel erstellen, löst VPC Resolver DNS-Abfragen für bestimmte Subdomänen auf, die andernfalls von DNS-Resolvern in Ihrem Netzwerk aufgelöst würden.

Standardmäßig gelten Weiterleitungsregeln für einen Domainnamen und alle entsprechenden Subdomains. Wenn Sie Abfragen für eine Domain an einen Resolver in Ihrem Netzwerk weiterleiten möchten, Abfragen für einige Subdomains hingegen nicht, erstellen Sie eine Systemregel für die Subdomains. Wenn Sie beispielsweise eine Weiterleitungsregel für example.com erstellen, Abfragen für acme.example.com jedoch nicht weiterleiten möchten, erstellen Sie eine Systemregel und geben für den Domainnamen acme.example.com an.

Delegierungsdatensatz — nur für die Delegiertenregel

DNS-Abfragen, die zu dieser Domain passen, werden an die Resolver in Ihrem Netzwerk weitergeleitet.

> **Note**
>
> Als Voraussetzung für eine Delegiertregel müssen Sie NS-Einträge in der privaten Hosting-Zone erstellen, wenn Sie eine private gehostete Zone für die ausgehende Delegierung verwenden. Der Datensatz lautet: NS — Nameserver zum Delegieren über den Resolver-Outbound-Endpunkt mit Delegate-Regel. Weitere Informationen finden Sie unter NS-Datensatztyp.

VPCs die diese Regel verwenden

Diejenigen VPCs , die diese Regel verwenden, um DNS-Abfragen für den oder die angegebenen Domainnamen weiterzuleiten. Sie können eine Regel auf VPCs beliebig viele anwenden.

Domainname — nur für die Weiterleitungsregel

DNS-Abfragen für diesen Domainnamen werden an die IP-Adressen weitergeleitet, die Sie in Target IP addresses (Ziel-IP-Adressen) festlegen. Sie können beispielsweise eine bestimmte Domain (example.com), eine Top-Level-Domain (com) oder einen Punkt (.) angeben, um alle DNS-Anfragen weiterzuleiten. Weitere Informationen finden Sie unter So bestimmt VPC Resolver, ob der Domainname in einer Abfrage irgendwelchen Regeln entspricht.

Ausgehender Endpunkt

VPC Resolver leitet DNS-Abfragen über den ausgehenden Endpunkt, den Sie hier angeben, an die IP-Adressen weiter, die Sie in Ziel-IP-Adressen angeben.

Ziel-IP-Adressen

Wenn eine DNS-Abfrage dem im Feld Domain name (Domainname) angegebenen Namen entspricht, leitet der ausgehende Endpunkt die Abfrage an die IP-Adressen weiter, die Sie hier angeben. Dies sind in der Regel die IP-Adressen für DNS-Resolver in Ihrem Netzwerk.

Target IP-Adressen (Ziel-IP-Adressen) ist nur verfügbar, wenn der Wert für Rule type (Regeltyp) Forward (Weiterleiten) lautet.

Geben Sie IPv4 unsere IPv6 Adressen und die Protokolle an, die ServerNameIndication Sie für den Endpunkt verwenden möchten. ServerNameIndication ist nur anwendbar, wenn das gewählte Protokoll DoH ist.

Das Auflösen der Ziel-IP-Adresse des FQDN eines DoH-Resolvers in Ihrem Netzwerk über den ausgehenden Endpunkt wird nicht unterstützt. Ausgehende Endpunkte benötigen die Ziel-IP-Adresse des DoH-Resolvers in Ihrem Netzwerk, an den die DoH-Anfragen weitergeleitet werden können. Wenn der DoH-Resolver in Ihrem Netzwerk den FQDN im TLS-SNI und im HTTP-Host-Header benötigt, muss dieser angegeben werden. ServerNameIndication

ServerNameIndication

Die Servernamensangabe des DoH-Servers, an den Sie Anfragen weiterleiten möchten. Dies wird nur verwendet, wenn das Protokoll DoH ist.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Dies sind die Tags, mit AWS Fakturierung und Kostenmanagement denen Sie Ihre AWS Rechnung organisieren können. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing - Benutzerhandbuch.

Verwalten von ausgehenden Endpunkten

Um ausgehende Endpunkte zu verwalten, führen Sie die entsprechenden Schritte aus.

Themen

Anzeigen und Bearbeiten von ausgehenden Endpunkten

Führen Sie zum Anzeigen und Bearbeiten von Einstellungen für einen ausgehenden Endpunkt die folgenden Schritte aus.

Anzeigen und Bearbeiten von Einstellungen für einen ausgehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Outbound endpoints (Ausgehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den ausgehenden Endpunkt erstellt haben.
4. Wählen Sie die Option für den Endpunkt, für den Sie Einstellungen anzeigen oder den Sie bearbeiten möchten.
5. Wählen Sie View details (Details anzeigen) oder Edit (Bearbeiten).

   Informationen zu den Werten für ausgehende Endpunkte finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.
6. Wenn Sie Edit (Bearbeiten) gewählt haben, geben Sie die entsprechenden Werte ein und klicken Sie anschließend auf Save (Speichern).

Anzeigen des Status für ausgehende Endpunkte

Gehen Sie folgendermaßen vor, um den Status eines ausgehenden Endpunkts anzuzeigen.

So zeigen Sie den Status eines ausgehenden Endpunkts an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Outbound endpoints (Ausgehende Endpunkte).

3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den ausgehenden Endpunkt erstellt haben. Die Spalte Status enthält einen der folgenden Werte:

   Erstellen

   VPC Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

   Betriebsbereit

   Die Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt sind korrekt konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und VPC Resolver weiterleiten.

   Aktualisieren

   VPC Resolver verknüpft oder trennt eine oder mehrere Netzwerkschnittstellen mit diesem Endpunkt.

   Automatische Wiederherstellung

   VPC Resolver versucht, eine oder mehrere der Netzwerkschnittstellen wiederherzustellen, die diesem Endpunkt zugeordnet sind. Während der Wiederherstellung funktioniert der Endpunkt aufgrund des Limits für die Anzahl der DNS-Abfragen pro IP-Adresse (pro Netzwerkschnittstelle) mit begrenzter Kapazität. Das aktuelle Limit finden Sie unter Kontingente auf Route 53 VPC Resolver.

   Aktion erforderlich

   Dieser Endpunkt ist fehlerhaft und VPC Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zugeordnet haben. Fügen Sie für jede IP-Adresse, die nicht verfügbar ist, eine andere IP-Adresse hinzu und löschen Sie dann die nicht verfügbare IP-Adresse. (Ein Endpunkt muss immer mindestens zwei IP-Adressen enthalten.) Ein Status von Aktion erforderlich kann verschiedene Ursachen haben. Hier sind zwei häufige Ursachen:

   - Eine oder mehrere Netzwerkschnittstellen, die diesem Endpunkt zugeordnet sind, wurden mit Amazon VPC gelöscht.
   - Die Netzwerkschnittstelle konnte aus einem Grund nicht erstellt werden, der nicht der Kontrolle von VPC Resolver unterliegt.

Löschen

VPC Resolver löscht diesen Endpunkt und die zugehörigen Netzwerkschnittstellen.

Löschen von ausgehenden Endpunkten

Bevor Sie einen Endpunkt löschen können, müssen Sie zunächst alle Regeln löschen, die einer VPC zugeordnet sind.

Gehen Sie wie folgt vor, um einen ausgehenden Endpunkt zu löschen.

> **Important**
>
> Wenn Sie einen ausgehenden Endpunkt löschen, beendet VPC Resolver die Weiterleitung von DNS-Anfragen von Ihrer VPC an Ihr Netzwerk für Regeln, die den gelöschten ausgehenden Endpunkt angeben.

So löschen Sie einen ausgehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Outbound endpoints (Ausgehende Endpunkte).
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie den ausgehenden Endpunkt erstellt haben.
4. Wählen Sie die Option für den Endpunkt, den Sie löschen möchten.
5. Wählen Sie Löschen aus.
6. Um zu bestätigen, dass Sie den Endpunkt löschen möchten, geben Sie den Namen des Endpunkts ein und wählen Sie dann Submit (Senden).

Verwalten von Weiterleitungsregeln

Wenn Sie möchten, dass VPC Resolver Abfragen für bestimmte Domainnamen an Ihr Netzwerk weiterleitet, erstellen Sie eine Weiterleitungsregel für jeden Domainnamen und geben den Namen der Domain an, für die Sie Abfragen weiterleiten möchten.

Themen

Anzeigen und Bearbeiten von Weiterleitungsregeln

Führen Sie zum Anzeigen und Bearbeiten einer Weiterleitungsregel die folgenden Schritte aus.

So können Sie Einstellungen für eine Weiterleitungsregel anzeigen und bearbeiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie die Option für die Regel, für die Sie Einstellungen anzeigen oder die Sie bearbeiten möchten.
5. Wählen Sie View details (Details anzeigen) oder Edit (Bearbeiten).

   Informationen zu den Werten für Weiterleitungsregeln finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.
6. Wenn Sie Edit (Bearbeiten) gewählt haben, geben Sie die entsprechenden Werte ein und klicken Sie anschließend auf Save (Speichern).

Erstellen von Weiterleitungsregeln

Führen Sie die folgenden Schritte aus, um eine oder mehrere Weiterleitungsregeln zu erstellen.

Um Weiterleitungsregeln zu erstellen und die Regeln einer oder mehreren zuzuordnen VPCs

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie Regel erstellen aus.
5. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.
6. Wählen Sie Save (Speichern) aus.
7. Um eine weitere Regel hinzuzufügen, wiederholen Sie die Schritte 4 bis 6.

Hinzufügen von Regeln für die umgekehrte Suche

Wenn Sie Reverse-Lookups in Ihrer VPC steuern müssen, können Sie dem ausgehenden Resolverendpunkt Regeln hinzufügen.

So erstellen Sie die Reverse-Lookup-Regel

1. Führen Sie die Schritte aus, die Sie bis zu Schritt 5 beschrieben haben.
2. Wenn Sie Ihre Regel angeben, geben Sie diePTR-Datensatz für die IP-Adresse oder die Adressen, für die Sie eine Reverse-Lookup-Weiterleitungsregel verwenden möchten.

   Wenn Sie beispielsweise Suchbegriffe für Adressen im Bereich 10.0.0.0/23 weiterleiten müssen, geben Sie zwei Regeln ein:

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

   Jede IP-Adresse in diesen Subnetzen wird als Subdomain dieser PTR-Datensätze referenziert, z. B. 10.0.1.161 hat die umgekehrte Lookup-Adresse 161.1.0.10.in-addr.apra, die eine Subdomain von 1.0.10.in-addra.apra ist.
3. Geben Sie den Server an, an den diese Suchbegriffe weitergeleitet werden sollen
4. Fügen Sie diese Regeln zu Ihrem ausgehenden Resolver-Endpunkt hinzu.

Beachten Sie, dass `enableDNSHostNames` für Ihre VPC fügt automatisch PTR-Datensätze hinzu. Siehe Was ist Route 53 VPC Resolver?. Das vorherige Verfahren ist nur erforderlich, wenn Sie explizit einen Resolver für bestimmte IP-Bereiche angeben möchten, z. B. beim Weiterleiten von Abfragen an einen Active Directory-Server.

Zuordnen von Weiterleitungsregeln zu einer VPC

Nachdem Sie eine Weiterleitungsregel erstellt haben, müssen Sie die Regel einer oder mehreren zuordnen VPCs. Die Regeln funktionieren erst, nachdem sie einer VPC zugeordnet wurden. Wenn Sie einer VPC eine Regel zuordnen, leitet VPC Resolver DNS-Abfragen für den in der Regel angegebenen Domänennamen an die DNS-Resolver weiter, die Sie in der Regel angegeben haben. Die Abfragen durchlaufen den ausgehenden Endpunkt, den Sie beim Erstellen der Regel angegeben haben.

Um eine Weiterleitungsregel einer oder mehreren zuzuordnen VPCs

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie den Namen der Regel, die Sie einer oder mehreren Regeln zuordnen möchten VPCs.
5. Wählen Sie Associate VPC (VPC zuordnen) aus.
6. Wählen Sie unter Diese Regel verwenden VPCs die Regel aus VPCs , der Sie die Regel zuordnen möchten.
7. Wählen Sie Hinzufügen aus.

Aufheben der Zuordnung der Weiterleitungsregeln zu einer VPC

Sie heben die Zuordnung einer Weiterleitungsregel zu einer VPC in den folgenden Fällen auf:

- Für DNS-Abfragen, die ihren Ursprung in dieser VPC haben, möchten Sie, dass VPC Resolver die Weiterleitung von Anfragen für den in der Regel angegebenen Domainnamen an Ihr Netzwerk beendet.
- Sie möchten die Weiterleitungsregel löschen. Wenn eine Regel derzeit einer oder mehreren Regeln zugeordnet ist VPCs, müssen Sie die Zuordnung der Regel zu allen Regeln aufheben, VPCs bevor Sie sie löschen können.

Wenn Sie die Zuordnung einer Weiterleitungsregel zu einer oder mehreren Regeln aufheben möchten VPCs, gehen Sie wie folgt vor.

So heben Sie die Zuordnung einer Weiterleitungsregeln zu einer VPC auf

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie den Namen der Regel aus, die Sie von einer oder mehreren VPCs Regeln trennen möchten.
5. Wählen Sie die Option für die VPC aus, von der Sie die Zuordnung der Regel trennen möchten.
6. Wählen Sie Disassociate (Zuordnung aufheben) aus.
7. Geben Sie zur Bestätigung Disassociate (Zuordnung aufheben) ein.
8. Wählen Sie Absenden aus.

Resolver-Regeln mit anderen AWS Konten teilen und gemeinsame Regeln verwenden

Sie können die Resolver-Regeln, die Sie mit einem AWS Konto erstellt haben, mit anderen AWS Konten teilen. Um Regeln gemeinsam zu nutzen, ist die Route 53 VPC Resolver-Konsole in AWS Resource Access Manager integriert. Weitere Informationen zu Resource Access Manager finden Sie im Benutzerhandbuch zu Resource Access Manager.

Beachten Sie Folgendes:

Verknüpfen von gemeinsamen Regeln mit VPCs

Wenn ein anderes AWS Konto eine oder mehrere Regeln mit Ihrem Konto geteilt hat, können Sie die Regeln Ihrem VPCs Konto zuordnen, genauso wie Sie Regeln verknüpfen, die Sie mit Ihrem VPCs erstellt haben. Weitere Informationen finden Sie unter Zuordnen von Weiterleitungsregeln zu einer VPC.

Löschen oder Aufheben der Freigabe einer Regel

Wenn Sie eine Regel mit anderen Konten teilen und dann entweder die Regel löschen oder die gemeinsame Nutzung beenden und wenn die Regel mit einem oder mehreren Konten verknüpft war VPCs, beginnt Route 53 VPC Resolver, DNS-Abfragen für diejenigen zu verarbeiten, die auf den verbleibenden Regeln VPCs basieren. Das Verhalten ist identisch mit dem Verhalten nach dem Aufheben der Zuordnung zu der VPC.

Wenn eine Regel für eine Organisationseinheit (OE) freigegeben ist und ein Konto in der OE in eine andere OE verschoben wird, werden alle Zuordnungen der freigegebenen Regel zu einem beliebigen VPC im Konto gelöscht. Wenn die VPC-Resolver-Regel jedoch bereits mit der Ziel-OU geteilt wurde, bleibt die VPC-Zuordnung erhalten und wird nicht getrennt.

Maximale Anzahl von Regeln und Zuordnungen

Wenn ein Konto eine Regel erstellt und sie mit einem oder mehreren anderen Konten gemeinsam nutzt, gilt die maximale Anzahl von Regeln pro AWS Region für das Konto, mit dem die Regel erstellt wurde.

Wenn ein Konto, für das eine Regel gemeinsam genutzt wird, die Regel mit einer oder mehreren verknüpft VPCs, gilt die maximale Anzahl von Verknüpfungen zwischen Regeln und VPCs pro Region für das Konto, mit dem die Regel geteilt wird.

Aktuelle VPC-Resolver-Kontingente finden Sie unter. Kontingente auf Route 53 VPC Resolver

Berechtigungen

Um eine Regel mit einem anderen AWS Konto zu teilen, benötigen Sie die Berechtigung, die PutResolverRulePolicyAktion zu verwenden.

Einschränkungen für das AWS Konto, mit dem eine Regel geteilt wird

Das Konto, für das eine Regel freigegeben werden, kann die Regel nicht ändern oder löschen.

Tagging

Nur das Konto, das eine Regel erstellt hat, kann Tags zu dieser hinzufügen, löschen oder anzeigen.

Führen Sie die folgenden Schritte aus, um den aktuellen Freigabestatus einer Regel (einschließlich des Kontos, das die Regel freigegeben hat, oder des Kontos, für das eine Regel freigegeben wurde) anzuzeigen und um Regeln für ein anderes Konto freizugeben.

Um den Freigabestatus und die Regeln für das Teilen mit einem anderen AWS Konto einzusehen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.

Die Spalte Sharing status (Freigabestatus) zeigt den aktuellen Freigabestatus der Regeln, die von dem aktuellen Konto erstellt wurden oder die für das aktuelle Konto freigegeben wurden:

- Nicht geteilt: Das aktuelle AWS Konto hat die Regel erstellt, und die Regel wird nicht mit anderen Konten geteilt.
- Shared by me (Von mir freigegeben): Das aktuelle Konto hat die Regel erstellt und für ein oder mehrere Konten freigegeben.
- Shared with me (Für mich freigegeben): Ein anderes Konto hat die Regel erstellt und für das aktuelle Konto freigegeben.

4. Wählen Sie den Namen der Regel, für die Sie Freigabeinformationen anzeigen möchten oder die Sie für ein anderes Konto freigeben möchten.

   Auf der *rule name* Seite Regel: zeigt der Wert unter Besitzer die ID des Kontos an, mit dem die Regel erstellt wurde. Dies ist das aktuelle Konto, sofern der Wert unter Sharing Status (Freigabestatus) nicht Shared with me (Für mich freigegeben) lautet. In diesem Fall handelt es sich bei Owner (Eigentümer) um das Konto, das die Regel erstellt und für das aktuelle Konto freigegeben hat.

5. Wählen Sie Share (Freigeben), um zusätzliche Informationen anzuzeigen oder die Regel für ein anderes Konto freizugeben. Je nach dem Wert unter Sharing status (Freigabestatus) wird eine der folgenden Seite in der Resource Access Manager-Konsole angezeigt:

   - Not shared (Nicht freigegeben): Die Seite Create resource share (Ressourcenfreigabe erstellen) wird angezeigt. Informationen zur Freigabe der Regel für ein anderes Konto, eine andere Organisationseinheit oder Organisation, finden Sie unter Schritt 6 beschrieben.
   - Shared by me (Von mir freigegeben): Die Seite Shared resources (Freigegebene Ressourcen) zeigt die Regeln und andere Ressourcen, die zu dem aktuellen Konto gehören und für andere Konten freigegeben wurden.
   - Shared with me (Für mich freigegeben): Die Seite Shared resources (Freigegebene Ressourcen) zeigt die Regeln und andere Ressourcen, die zu anderen Konten gehören und für das aktuelle Konto freigegeben wurden.

6. Um eine Regel mit einem anderen AWS Konto, einer anderen Organisationseinheit oder Organisation zu teilen, geben Sie die folgenden Werte an.

> **Note**
>
> Sie können keine Freigabeeinstellungen aktualisieren. Wenn Sie eine der folgenden Einstellungen ändern möchten, müssen Sie eine Regel mit den neuen Einstellungen freigeben und die alten Freigabeeinstellungen anschließend entfernen.

Description

Geben Sie eine Kurzbeschreibung ein, mit der Sie sich den Grund für die Freigabe der Regel merken können.

Ressourcen

Aktivieren Sie das Kontrollkästchen für die Regel, die Sie freigeben möchten.

Prinzipale

Geben Sie die AWS Kontonummer, den Namen der Organisationseinheit oder den Namen der Organisation ein.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Dies sind die Tags, mit AWS Fakturierung und Kostenmanagement denen Sie Ihre AWS Rechnung organisieren können. Sie können Tags auch für andere Zwecke verwenden. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

Löschen von Weiterleitungsregeln

Gehen Sie wie folgt vor, um eine Weiterleitungsregel zu löschen.

Beachten Sie Folgendes:

- Wenn die Weiterleitungsregel einer Regel zugeordnet ist VPCs, müssen Sie die Verknüpfung zwischen der Regel und der Regel trennen, VPCs bevor Sie die Regel löschen können. Weitere Informationen finden Sie unter Aufheben der Zuordnung der Weiterleitungsregeln zu einer VPC.

- Sie können die Standardregel Internet-Resolver nicht löschen, die einen Wert von Recursive für Type hat. Diese Regel bewirkt, dass Route 53 VPC Resolver als rekursiver Resolver für alle Domainnamen fungiert, für die Sie keine benutzerdefinierten Regeln erstellt haben und für die VPC Resolver keine automatisch definierten Regeln erstellt hat. Weitere Informationen darüber, wie Regeln kategorisiert werden, finden Sie unter Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden.

So löschen Sie eine Weiterleitungsregel

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.
4. Wählen Sie die Option für die Regel, die Sie löschen möchten.
5. Wählen Sie Löschen aus.
6. Um zu bestätigen, dass Sie die Regel löschen möchten, geben Sie den Namen der Regel ein und wählen Sie Submit (Senden).

Weiterleitungsregeln für Reverse-DNS-Abfragen in VPC Resolver

Wenn die `enableDnsHostnames` und `true` für eine Virtual Private Cloud (VPC) von Amazon VPC auf gesetzt `enableDnsSupport` sind, erstellt VPC Resolver automatisch automatisch definierte Systemregeln für Reverse-DNS-Abfragen. Weitere Informationen zu diesen Einstellungen finden Sie unter DNS-Attribute in Ihrem VPCim Entwicklerhandbuch für Amazon VPC.

Weiterleitungsregeln für Reverse-DNS-Abfragen sind besonders nützlich für Dienste wie SSH oder Active Directory, die in der Lage sind, Benutzer zu authentifizieren, indem sie eine Reverse-DNS-Suche nach der IP-Adresse durchführen, von der aus ein Kunde versucht, eine Verbindung zu einer Ressource herzustellen. Weitere Informationen zu automatisch definierten Systemregeln finden Sie unter Domainnamen, für die VPC Resolver automatisch definierte Systemregeln erstellt.

Sie können diese Regeln deaktivieren und alle Reverse-DNS-Abfragen so ändern, dass sie beispielsweise zur Lösung an Ihre On-Premises-Nameserver weitergeleitet werden.

Nachdem Sie die automatischen Regeln deaktiviert haben, erstellen Sie Regeln, um die Abfragen nach Bedarf an Ihre On-Premises-Ressourcen weiterzuleiten. Weitere Informationen über die Verwaltung von Weiterleitungsregeln finden Sie unter Verwalten von Weiterleitungsregeln.

So deaktivieren Sie automatisch definierte Regeln

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen VPCsSie im Navigationsbereich unter VPC Resolver und anschließend eine VPC-ID aus.
3. Deaktivieren Sie das Kontrollkästchen unter Autodefined rules for reverse DNS resolution (Automatisch definierte Regeln für die umgekehrte DNS-Auflösung). Wenn das Kontrollkästchen bereits deaktiviert ist, können Sie es auswählen, um die automatisch definierte Reverse-DNS-Auflösung zu aktivieren.

Weitere Informationen finden Sie APIs unter Konfiguration des VPC-Resolvers. APIs

Tutorial zu Resolver-Delegierungsregeln

Die Delegierungsregel ermöglicht es dem VPC-Resolver, die Nameserver, die die delegierte Zone hosten, über den angegebenen ausgehenden Endpunkt zu erreichen. Während die Weiterleitungsregel den VPC-Resolver darüber informiert, die DNS-Anfragen über den ausgehenden Endpunkt an die Nameserver weiterzuleiten, die der angegebenen Domain entsprechen, informiert die Delegierungsregel den VPC Resolver, die delegierten Nameserver über den ausgehenden Endpunkt zu erreichen, der bei der Rückgabe der delegierten NS-Einträge angegeben wurde. VPC Resolver sendet eine Anfrage an die delegierten Nameserver, wenn die NS-Einträge in der DNS-Antwort mit dem im Delegierungseintrag angegebenen Domainnamen übereinstimmen.

Schritte zur Verwendung der ausgehenden Delegierung des Resolver-Endpunkts

1. Erstellen Sie einen ausgehenden Resolver-Endpunkt in der VPC, von dem aus DNS-Abfragen an die Resolver in Ihrem Netzwerk gesendet werden sollen.

   Sie können entweder die folgende API oder den CLI-Befehl verwenden:

   - `CreateResolverEndpoint-API`
   - `create-resolver-endpoint-CLI`
2. Erstellen Sie eine oder mehrere Delegierungsregeln, die die Domainnamen angeben, für die die Abfragen über den angegebenen ausgehenden Endpunkt an Ihr Netzwerk delegiert werden sollen.

Beispiel für die Erstellung einer Delegierungsregel mit CLI:

```
aws route53resolver create-resolver-rule \
--region REGION \
--creator-request-id delegateruletest \
--delegation-record example.com \
--name delegateruletest \
--rule-type DELEGATE \
--resolver-endpoint-id outbound endpoint ID
```

3. Ordnen Sie die Delegierungsregel der Regel zu, VPCs für die Sie die Abfragen delegieren möchten.

   Sie können entweder die folgende API oder den CLI-Befehl verwenden:

   - AssociateResolverRuleAPI.
   - associate-resolver-rulesCLI-Befehl.

Arten der Delegierung, die vom ausgehenden Resolver-Endpunkt unterstützt werden

VPC Resolver unterstützt zwei Arten der ausgehenden Delegierung:

- Leiten Sie die private gehostete Zone 53 an die ausgehende VPC Resolver-Delegierung weiter:

  Delegiert mithilfe der ausgehenden Delegierung eine Subdomain von einer privaten Hosting-Zone entweder an einen lokalen DNS-Server oder eine öffentliche gehostete Zone im Internet. Diese ausgehende Delegierung ermöglicht es Ihnen, die Verwaltung Ihrer DNS-Einträge zwischen der privaten Hosting-Zone und der delegierten Zone aufzuteilen. Die Delegierung kann mit oder ohne Glue-Record in einer privaten Hosting-Zone erfolgen, je nach Ihrem DNS-Setup. Weitere Informationen finden Sie unter. Private gehostete Zone für ausgehenden Datenverkehr
- Delegierung von ausgehender zu ausgehender VPC Resolver:

  Delegiert eine Subdomain von Ihrem lokalen DNS-Server an einen anderen lokalen Server an demselben oder einem anderen Standort mithilfe der Delegierung von ausgehendem zu ausgehendem Datenverkehr. Dies ist vergleichbar mit der Delegierung von einer privaten gehosteten Zone an einen ausgehenden Endpunkt, wo Sie an eine Zone delegieren können, die

auf Ihrem lokalen Nameserver gehostet wird. Weitere Informationen finden Sie unter Ausgehend bis ausgehend.

Beispiel für eine Konfiguration für die ausgehende Delegierung von Route 53 an die private gehostete Zone von VPC Resolver

Gehen wir von einem DNS-Setup aus, bei dem die übergeordnete gehostete Zone in einer privaten Hosting-Zone auf Route 53 in einer Amazon-VPC gehostet wird und Subdomains an Nameserver delegiert werden, die in Europa, Asien und Nordamerika gehostet werden. Alle DNS-Abfragen werden über den VPC Resolver weitergeleitet.

Folgen Sie den Beispielschritten, um Ihre private gehostete Zone und Ihren VPC-Resolver zu konfigurieren.

Konfigurieren Sie die private gehostete Zone für die ausgehende Delegierung

1. Für die Einrichtung der privaten gehosteten Zone:

   Übergeordnete gehostete Zone: `hr.example.com`

```
$TTL    86400 ; 24 hours
$ORIGIN hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of Zone Delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue Record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue Record
```

2. Für den lokalen Nameserver in der lokalen Region Europa:

   - Gehostete Zone: `eu.hr.example.com` NS IP: `10.0.0.30`

```
$TTL    86400 ; 24 hours
$ORIGIN eu.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
```

```
test.eu.hr.example.com IN A 1.2.3.4
```

3. Für den lokalen Nameserver in der lokalen Region Asien:

   Gehostete Zone:, `apac.hr.example.com` `10.0.0.40`

   Der APAC-Nameserver kann die Subdomain an andere Nameserver delegieren.

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

   Gehostete Zone:, `engineering.apac.hr.example.com` `10.0.0.80`

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Für den lokalen Nameserver in der lokalen Region Nordamerika:

   Gehostete Zone: `na.hr.example.net` NS IP: `10.0.0.50`

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

Einrichtung des VPC-Resolvers

- Für den VPC Resolver müssen Sie eine Weiterleitungsregel und zwei Delegierungsregeln einrichten:

  Weiterleitungsregel

  1. Für die Weiterleitung des out-of-zone Delegierungsdatensatzes, sodass der Route 53 VPC Resolver die IP des delegierten NS kennt, um die erste Anfrage weiterzuleiten.

     Domänenname: Ziel-IPs: `hr.example.net` `10.0.0.50`

  Regeln für die Delegierung

  1. Delegierungsregel für die Delegierung innerhalb der Zone:

     Delegationsdatensatz: `hr.example.com`
  2. Delegierungsregel für die Delegierung außerhalb der Zone:

     Delegationsdatensatz: `hr.example.net`

Beispielkonfiguration für die Delegierung von ausgehendem zu ausgehendem Datenverkehr

Anstatt die übergeordnete gehostete Zone in einer Amazon-VPC zu haben, gehen wir von einem DNS-Setup aus, bei dem sich die übergeordnete gehostete Zone am zentralen lokalen Standort befindet und Subdomains an Nameserver delegiert werden, die in Europa, Asien und Nordamerika gehostet werden. Alle DNS-Abfragen werden über den VPC Resolver weitergeleitet.

Folgen Sie den Beispielschritten, um Ihr lokales DNS und den VPC-Resolver zu konfigurieren.

Konfigurieren Sie On-Premise-DNS

1. Für den lokalen Nameserver in der zentralen lokalen Region:

   - Übergeordnete gehostete Zone: `hr.example.com`

     Gehostete Zone`hr.example.com`, NS-IP: `10.0.0.20`

```
$TTL    86400 ; 24 hours
$ORIGIN hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
eu.hr.example.com IN NS ns1.eu.hr.example.com.
apac.hr.example.com IN NS ns2.apac.hr.example.com.
na.hr.example.com IN NS ns3.na.hr.example.net. # Out of zone delegation

ns1.eu.hr.example.com IN A 10.0.0.30 # Glue record
ns2.apac.hr.example.com IN A 10.0.0.40 # Glue record
```

2. Für den lokalen Nameserver in der lokalen Region Europa (die Konfiguration für die Nameserver Europa, Asien und Nordamerika ist dieselbe wie für die private gehostete Zone zur ausgehenden Delegierung):

   - Gehostete Zone: NS IP: `eu.hr.example.com` `10.0.0.30`

```
$TTL    86400 ; 24 hours
$ORIGIN eu.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.eu.hr.example.com IN A 1.2.3.4
```

3. Für den lokalen Nameserver in der lokalen Region Asien:

   Gehostete Zone:, `apac.hr.example.com` `10.0.0.40`

   Der APAC-Nameserver kann die Subdomain an andere Nameserver delegieren.

```
$TTL    86400 ; 24 hours
$ORIGIN apac.hr.example.com
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @

test.apac.hr.example.com IN A 5.6.7.8
engineering.apac.hr.example.com IN NS ns1.engineering.apac.hr.example.com
sales.apac.hr.example.com IN NS ns2.sales.apac.hr.example.com
ns1.engineering.apac.hr.example.com IN A 10.0.0.80
```

```
ns2.sales.apac.hr.example.com IN A 10.0.0.90
```

Gehostete Zone:, `engineering.apac.hr.example.com` `10.0.0.80`

```
$TTL 86400 ; 24 hours
$ORIGIN engineering.apac.hr.example.com
@ 1D IN SOA @ root (20200322001 3H 15 1w 3h)
@ 1D IN NS @
test.engineering.apac.hr.example.com IN A 1.1.1.1
```

4. Für den lokalen Nameserver in der lokalen Region Nordamerika:

   Gehostete Zone: `na.hr.example.net` NS IP: `10.0.0.50`

```
$TTL    86400 ; 24 hours
$ORIGIN na.hr.example.net
@  1D  IN     SOA @    root (20200322001 3H 15 1w 3h)
@  1D  IN  NS @
ns3.na.hr.example.net. IN A 10.0.0.50
test.na.hr.example.com  IN A 9.10.11.12
```

Einrichtung des VPC-Resolvers

- Für den VPC Resolver müssen Sie Weiterleitungsregeln und Delegierungsregeln einrichten:

  Regeln weiterleiten

  1. Gehen Sie wie folgt vor, um die ursprüngliche Anfrage weiterzuleiten, sodass die Anfragen an die übergeordnete gehostete Zone `hr.example.com` am zentralen Standort weitergeleitet werden:

     Domänenname: Ziel-IPs: `hr.example.com` `10.0.0.20`

  2. Für die Weiterleitung des out-of-zone Delegierungsdatensatzes, sodass der VPC Resolver die IP-Adresse des delegierten Nameservers kennt, um die erste Anfrage weiterzuleiten:

     Domänenname: Ziel-IPs: `hr.example.net` `10.0.0.50`

  Regeln für die Delegierung

  1. Delegierungsregel für die Delegierung innerhalb der Zone:

Delegierungsdatensatz: `hr.example.com`

2. Delegierungsregel für die Delegierung außerhalb der Zone:

   Delegationsdatensatz: `hr.example.net`

Aktivieren der DNSSEC-Validierung in Amazon Route 53

Wenn Sie die DNSSEC-Validierung für eine Virtual Private Cloud (VPC) in Amazon Route 53 aktivieren, werden DNSSEC-Signaturen kryptografisch überprüft, um sicherzustellen, dass die Antwort nicht manipuliert wurde. Sie aktivieren die DNSSEC-Validierung auf Ihrer VPC Detailseite.

Die DNSSEC-Validierung wird von VPC Resolver auf öffentlich signierte Namen angewendet, wenn er eine rekursive DNS-Auflösung durchführt.

Wenn der VPC-Resolver jedoch an einen anderen DNS-Resolver weiterleitet, führt dieser Resolver eine rekursive DNS-Auflösung durch und muss daher auch die DNSSEC-Validierung anwenden.

Important

Die Aktivierung der DNSSEC-Validierung kann sich auf die DNS-Auflösung für öffentliche DNS-Einträge aus AWS -Ressourcen in einer VPC, was zu einem Nutzungsausfall führen könnte. Beachten Sie, dass die Aktivierung oder Deaktivierung der DNSSEC-Validierung einige Minuten dauern kann.

Note

Derzeit ignoriert der Route 53 VPC Resolver in Ihrer VPC (auch bekannt als AmazonProvided DNS) das DO (DNSSEC OK) EDNS-Header-Bit und das CD-Bit (Checking Disabled) in der DNS-Abfrage. Wenn Sie DNSSEC konfiguriert haben, bedeutet dies, dass der VPC-Resolver zwar eine DNSSEC-Validierung durchführt, aber weder DNSSEC-Einträge zurückgibt noch das AD-Bit in der Antwort festlegt. Daher wird die Durchführung Ihrer eigenen DNSSEC-Validierung derzeit vom VPC Resolver nicht unterstützt. Wenn Sie dies ausführen müssen, müssen Sie Ihre eigene rekursive DNS-Auflösung durchführen.

So aktivieren Sie die DNSSEC-Validierung für eine VPC

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im Navigationsbereich unter VPC Resolver die Option. VPCs
3. Aktivieren Sie das Kontrollkästchen unter DNSSEC-Validierung. Wenn das Kontrollkästchen bereits aktiviert ist, können Sie es deaktivieren, um die DNSSEC-Validierung zu deaktivieren.

   Beachten Sie, dass die Aktivierung oder Deaktivierung der DNSSEC-Validierung einige Minuten dauern kann.

Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen

Sie können Amazon Route 53 verwenden, um den Verkehr an eine Vielzahl von AWS Ressourcen weiterzuleiten.

- Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens
- Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens
- Traffic an eine EC2 Amazon-Instance weiterleiten
- Weiterleiten des Datenverkehrs an einen AWS App Runner Dienst
- Weiterleiten des Datenverkehrs zu einem AWS Global Accelerator
- Weiterleiten des Datenverkehrs an eine AWS Elastic Beanstalk Umgebung
- Weiterleiten von Datenverkehr an einen ELB Load Balancer
- Weiterleiten von Datenverkehr an eine Website, die in einem Amazon-S3-Bucket gehostet wird.
- Weiterleiten des Datenverkehrs an einen Amazon-Virtual-Private Cloud-Schnittstellenendpunkt unter Verwendung Ihres Domainnamens
- Weiterleitung des Datenverkehrs an Amazon WorkMail
- Weiterleitung des Datenverkehrs an den Amazon OpenSearch Service-Domänenendpunkt
- Weiterleiten des Datenverkehrs an den Domänenendpunkt des Amazon VPC Lattice-Dienstes
- Weiterleiten des Datenverkehrs an andere AWS Ressourcen
- Erstellen von Amazon Route 53- und Route 53 VPC Resolver-Ressourcen mit AWS CloudFormation

Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens

Sie können Amazon API Gateway verwenden, um zu erstellen, zu veröffentlichen, zu verwalten, zu überwachen und zu sichern APIs. Sie können zusätzlich zu APIs den in der AWS Cloud gespeicherten Daten auch Dienste für den Zugriff AWS oder andere Webdienste erstellen.

Die Methode, die Sie zum Weiterleiten des Domaindatenverkehrs an eine API-Gateway-API verwenden, ist dieselbe, unabhängig davon, ob Sie einen regionalen API-Gateway-Endpunkt

oder einen Edge-optimierten API-Gateway-Endpunkt erstellt haben. Wenn Sie einen privaten API-Gateway-Endpunkt erstellen, unterscheidet sich der Vorgang geringfügig.

- Regionaler API-Endpunkt: Sie erstellen einen Route-53-Aliasdatensatz, der den Datenverkehr an den regionalen API-Endpunkt weiterleitet.
- Edge-optimierter API-Endpunkt: Sie erstellen einen Route-53-Aliasdatensatz, der den Datenverkehr an die Edge-optimierte API weiterleitet. Dadurch wird der Datenverkehr an die CloudFront Distribution weitergeleitet, die der Edge-optimierten API zugeordnet ist.
- Privater API-Endpunkt: Sie erstellen einen Route 53-Aliaseintrag, der den Datenverkehr mithilfe eines Schnittstellen-VPC-Endpunkts für API Gateway in einer privaten gehosteten Zone an Ihren privaten API-Endpunkt weiterleitet.

Ein Aliasdatensatz ist eine Route-53-Erweiterung für DNS, die einem CNAME-Datensatz ähnelt. Einen Vergleich von Alias- und CNAME-Datensätzen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

> **Note**
>
> Route 53 berechnet keine Gebühren für Aliasabfragen an API Gateway APIs oder andere AWS Ressourcen.

Themen

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Eine API-Gateway-API, die einen benutzerdefinierten Domainnamen hat (z. B. „api.example.com“), der mit dem Namen des zu erstellenden Route-53-Datensatzes übereinstimmt.

  Weitere Informationen finden Sie unter den folgenden Themen:

  - Einrichtung benutzerdefinierter Domainnamen für HTTP APIs im Amazon API Gateway Developer Guide.

- Einrichtung benutzerdefinierter Domainnamen für REST APIs im Amazon API Gateway Developer Guide.
- Einrichtung benutzerdefinierter Domainnamen für WebSocket APIs im Amazon API Gateway Developer Guide.
- Benutzerdefinierte Domainnamen für private APIs in API Gateway im Amazon API Gateway Developer Guide.

- Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfigurieren von Route 53 zur Weiterleitung des Datenverkehrs an einen API-Gateway-Endpunkt

Zum Konfigurieren von Route 53 zur Weiterleitung des Datenverkehrs an einen API-Gateway-Endpunkt führen Sie die folgenden Schritte aus.

Custom domain names for public APIs

Das folgende Verfahren beschreibt, wie der Datenverkehr für einen benutzerdefinierten Domainnamen für die Öffentlichkeit an einen API-Gateway-Endpunkt weitergeleitet wird APIs.

So leiten Sie Datenverkehr an einen API-Gateway-Endpunkt weiter

1. Wenn Sie die gehostete Route-53-Zone und den Endpunkt mit demselben Konto erstellt haben, fahren Sie mit Schritt 2 fort.

   Wenn Sie die gehostete Zone und den Endpunkt mit verschiedenen Konten erstellt haben, erhalten Sie den Zieldomainnamen für den benutzerdefinierten Domainnamen, den Sie verwenden möchten:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die API Gateway Gateway-Konsole unter https://console.aws.amazon.com/apigateway/.

b. Wählen Sie im Navigationsbereich Custom Domain Namens (Benutzerdefinierte Domainnamen).

c. Wählen Sie den benutzerdefinierten Domainnamen, den Sie verwenden möchten und erhalten Sie den Wert von API-Gateway-Domainname.

2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie den Namen der gehosteten Zone, die den zu verwendenden Domainnamen hat, um den Datenverkehr an Ihre API weiterzuleiten.
5. Wählen Sie Datensatz erstellen.
6. Geben Sie die folgenden Werte an:

> **Important**
>
> Wir empfehlen, Alias zu aktivieren. Bei Domainnamen, die keinen Route 53-Aliaseintrag verwenden, können Probleme auftreten, wenn Sie eine VPC mit aktiviertem privaten DNS verwenden, um eine private API aufzurufen. Private DNS überschreibt das standardmäßige DNS-Auflösungsverhalten innerhalb der VPC, was zu Konflikten mit externen DNS-Einträgen führen kann.

Routing-Richtlinie

Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an die API zu leiten.

Die API, an die Sie Datenverkehr leiten möchten, muss einen benutzerdefinierten Domainnamen haben (z. B. „api.example.com“), der mit dem Namen des zu erstellenden Route-53-Datensatzes übereinstimmt.

Alias

Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias zu API-Gateway-API und dann die Region aus, aus der der Endpunkt stammt.

Wie Sie den Wert für Endpoint angeben, hängt davon ab, ob Sie die gehostete Zone und die API mit demselben AWS Konto oder mit unterschiedlichen Konten erstellt haben:

- Gleiches Konto — Die Liste der Zieldomänennamen enthält nur solche APIs mit einem benutzerdefinierten Domainnamen, der dem Wert entspricht, den Sie für Datensatzname angegeben haben. Wählen Sie einen geeigneten Wert aus.
- Unterschiedliche Konten – Geben Sie den Wert ein, den Sie in Schritt 1 dieser Vorgehensweise erhalten haben.

Datensatztyp

Wählen Sie eine — IPv4 Adresse.

Evaluate Target Health

Konfigurieren Sie benutzerdefinierte Zustandsprüfungen, um das DNS-Failover zu kontrollieren. Ein Beispiel finden Sie unter Konfigurieren von benutzerdefinierten Zustandsprüfungen für DNS-Failover im API-Gateway-Benutzerhandbuch.

7. Wählen Sie Create records (Datensätze erstellen).

   Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an die API leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Custom domain names for private APIs

Das folgende Verfahren beschreibt, wie der Datenverkehr für einen benutzerdefinierten Domainnamen für private Benutzer an einen API-Gateway-Endpunkt weitergeleitet wird APIs.

So leiten Sie Datenverkehr an einen API-Gateway-Endpunkt weiter

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

3. Wählen Sie den Namen der privaten gehosteten Zone mit dem Domainnamen aus, den Sie für die Weiterleitung von Datenverkehr an Ihre API verwenden möchten.
4. Wählen Sie Datensatz erstellen.
5. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

   Datensatzname

   Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an die API zu leiten.

   Die API, an die Sie Datenverkehr leiten möchten, muss einen benutzerdefinierten Domainnamen haben (z. B. „api.example.com“), der mit dem Namen des zu erstellenden Route-53-Datensatzes übereinstimmt.

   Alias

   Schalten Sie Alias ein.

   Bewerten/Weiterleiten des Datenverkehrs an

   Wählen Sie Alias to VPC Endpoint. Wählen Sie die Region aus, aus der der Endpunkt stammt, und wählen Sie dann Ihren VPC-Endpunkt aus.

   Datensatztyp

   Wenn Sie IPv6 für Ihren VPC-Endpunkt verwenden, erstellen Sie einen AAAA-Eintragstyp. Wenn Sie Dualstack für Ihren VPC-Endpunkt verwenden, erstellen Sie sowohl einen AAAA- als auch einen A-Datensatztyp.

   Evaluate Target Health

   Konfigurieren Sie benutzerdefinierte Zustandsprüfungen, um das DNS-Failover zu kontrollieren. Ein Beispiel finden Sie unter Konfigurieren von benutzerdefinierten Zustandsprüfungen für DNS-Failover im API-Gateway-Benutzerhandbuch.
6. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an

die API leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens

Dieses Thema enthält umfassende Verfahren für die Weiterleitung von DNS-Verkehr an eine beliebige CloudFront Amazon-Distribution. Wenn Sie eine statische Website mit Amazon CloudFront und Amazon Simple Storage Service einrichten, finden Sie Verwenden Sie eine CloudFront Amazon-Distribution, um eine statische Website bereitzustellen ein vollständiges Tutorial unter.

Sie können Amazon CloudFront, das AWS Content Delivery Network (CDN), als eine Möglichkeit verwenden, die Bereitstellung Ihrer Webinhalte zu beschleunigen. CloudFront kann Ihre gesamte Website — einschließlich dynamischer, statischer, gestreamter und interaktiver Inhalte — mithilfe eines globalen Netzwerks von Edge-Standorten bereitstellen. Benutzer, die Ihre Inhalte anfordern, werden automatisch an den Edge-Standort weitergeleitet, der die niedrigste Latenz für sie aufweist.

> **Note**
>
> Sie können den Traffic nur für öffentlich gehostete Zonen an eine CloudFront Distribution weiterleiten.

Um die Inhalte Ihrer Website CloudFront zu verteilen, erstellen Sie eine Verteilung und geben Sie die entsprechenden Einstellungen an. Geben Sie beispielsweise den Amazon S3 S3-Bucket oder den HTTP-Server CloudFront an, von dem Sie Ihre Inhalte abrufen möchten, ob nur ausgewählte Benutzer Zugriff auf Ihre Inhalte haben sollen und ob Sie möchten, dass Benutzer HTTPS verwenden.

Wenn Sie eine Distribution erstellen, CloudFront weist Sie der Distribution einen Domainnamen zu, z. B. d111111abcdef8.cloudfront.net Sie können diesen Domainnamen in der URLs für Ihre Inhalte verwenden, zum Beispiel:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Alternativ können Sie Ihren eigenen Domainnamen verwenden URLs, zum Beispiel in:

```
http://example.com/logo.jpg
```

Folgen Sie den Schritten im Amazon CloudFront Developer Guide, um Ihren eigenen Domainnamen in Ihren Dateien URLs in einer CloudFront Distribution zu verwenden, anstatt den Domainnamen, der Ihrer Distribution CloudFront zugewiesen wurde. Weitere Informationen zur Verwendung Ihres eigenen Domainnamens bei einer CloudFront Distribution finden Sie unter Benutzerdefiniert verwenden, URLs indem Sie alternative Domainnamen hinzufügen () CNAMEs.

Wenn Sie einen Route 53-Domainnamen mit einer CloudFront Verteilung verwenden, verwenden Sie Amazon Route 53, um einen Aliaseintrag zu erstellen, der auf Ihre CloudFront Verteilung verweist. Ein Alias-Datensatz ist eine Route-53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomain (z. B. example.com) als auch für Subdomains (z. B. www.example.com) verwenden. (Sie können CNAME-Datensätze nur für Subdomains erstellen.) Wenn Route 53 eine DNS-Abfrage mit dem angegebenen Namen und Typ eines Alias-Datensatzes erhält, antwortet mit dem Domainnamen, der Ihrer Verteilung zugeordnet ist.

> **Note**
>
> Route 53 erhebt keine Gebühren für Alias-Abfragen an CloudFront Distributionen oder andere AWS Ressourcen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

1. Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
2. Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

   Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter für Ihre Domain finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.
3. Ein CloudFront Vertriebs- oder CloudFront Distributionsmandant. Die Verteilung muss einen alternativen Domainnamen enthalten, der dem Domainnamen entspricht, den Sie für Ihre Distribution verwenden möchten, und URLs nicht dem Domainnamen, CloudFront der Ihrer Distribution zugewiesen wurde. Für einen CloudFront Distributionsmandanten muss sie den Domainnamen enthalten, den Sie für Ihren verwenden möchten URLs.

Wenn Sie beispielsweise möchten, dass Ihr Inhalt den URLs Domainnamen example.com enthält, muss das Feld Alternativer Domainname für die Verteilung example.com enthalten.

Weitere Informationen finden Sie in der folgenden Dokumentation im Amazon CloudFront Developer Guide:

- Aufgabenliste für die Erstellung einer Verteilung
- Erstellen oder Aktualisieren einer Verteilung mithilfe der CloudFront-Konsole

> **Note**
>
> Wenn Sie eine statische Website erstellen, finden Sie unter Erste Schritte mit einer sicheren statischen Website im Amazon CloudFront Developer Guide eine vollständige Anleitung zur Einrichtung.

4. (Optional) Fordern Sie ein öffentliches Zertifikat an, damit CloudFront Amazon-Distributionen HTTPS erfordern. Weitere Informationen finden Sie unter DNS-Validierung im AWS Certificate Manager im AWS Certificate Manager -Benutzerhandbuch.

Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an eine CloudFront Verteilung

Gehen Sie wie folgt vor, um Amazon Route 53 so zu konfigurieren, dass der Verkehr an eine CloudFront Verteilung weitergeleitet wird. Weitere Informationen zur Verwendung Ihres eigenen Domainnamens bei einer CloudFront Distribution finden Sie unter Benutzerdefiniert verwenden, URLs indem Sie alternative Domainnamen hinzufügen (CNAMEs) im Amazon CloudFront Developer Guide.

> **Note**
>
> Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Änderungen übernommen werden, können Sie Traffic an Ihre CloudFront Distribution weiterleiten, indem Sie den Namen des Alias-Eintrags verwenden, den Sie in diesem Verfahren erstellen.

So leiten Sie Datenverkehr an die CloudFront -Verteilung weiter

1. Rufen Sie den Domainnamen ab, CloudFront der Ihrer Distribution zugewiesen wurde, und stellen Sie fest, ob er aktiviert IPv6 ist:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudFront Konsole unterhttps://console.aws.amazon.com/cloudfront/v4/home.

   b. Wählen Sie in der Spalte ID den verknüpften Namen der Verteilung aus, an die Sie den Datenverkehr weiterleiten möchten (nicht das Kontrollkästchen).

   c. Rufen Sie auf der Registerkarte General (Allgemein) den Wert aus dem Feld Distribution domain name (Name der Verteilungsdomain) ab.

   d. Wählen Sie auf der Registerkarte Allgemein im Abschnitt Einstellungen die Option Bearbeiten aus und blättern Sie, bis Sie das IPv6Feld überprüfen, um zu sehen, ob IPv6 es für die Verteilung aktiviert ist. Wenn diese Option aktiviert IPv6 ist, müssen Sie zwei Aliaseinträge für die Verteilung erstellen, einen, um den IPv4 Verkehr an die Verteilung weiterzuleiten, und einen, um den IPv6 Verkehr weiterzuleiten. Klicken Sie auf Abbrechen.

      Weitere Informationen finden Sie unter Aktivieren IPv6 im Thema Werte, die Sie angeben, wenn Sie eine Distribution erstellen oder aktualisieren, im Amazon CloudFront Developer Guide.

2. Für einen CloudFront Distributionsmandanten

   a. Wählen Sie in der linken Navigationsleiste SaaS, dann Distribution Tenants und wählen Sie den Distributionsmandanten mit dem Domainnamen aus, an den Sie den Traffic weiterleiten möchten

   b. Kopieren Sie im Abschnitt Allgemeine Details den Wert des Endpunkts.

3. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

4. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

5. Wählen Sie den verknüpften Namen der gehosteten Zone für die Domain aus, die Sie verwenden möchten, um den Traffic an Ihre CloudFront Distribution weiterzuleiten.

6. Wählen Sie Datensatz erstellen.

7. Geben Sie die folgenden Werte an:

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Traffic an Ihre CloudFront Distribution weiterzuleiten. Der Standardwert ist der Name der gehosteten Zone.

Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihre Verteilung zu leiten, geben Sie acme ein.

Datensatztyp

Wählen Sie eine — IPv4 Adresse.

Wenn für die Verteilung aktiviert IPv6 ist und Sie einen zweiten Datensatz erstellen, wählen Sie AAAA — IPv6 Adresse.

Alias

Schalten Sie Alias ein.

> **Important**
>
> Sie müssen einen Alias-Datensatz erstellen, damit die CloudFront Verteilung funktioniert.

Datenverkehr weiterleiten an

Wählen Sie Alias für die CloudFront Verteilung aus. Wählen Sie den Domainnamen, den Sie der Distribution bei der Erstellung CloudFront zugewiesen haben. Dies ist der Wert, den Sie in Schritt 1 erhalten haben.

Wählen Sie für einen CloudFront Verteilungsmandanten den Endpunkt aus Schritt 2 aus.

Evaluate Target Health

Übernehmen Sie den Standardwert No.

Routing-Richtlinie

Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

8. Wählen Sie Create records (Datensätze erstellen).
9. Wenn für die Verteilung aktiviert IPv6 ist, wiederholen Sie die Schritte 5 bis 7. Geben Sie die gleichen Einstellungen an, außer für das Feld Datensatztyp, wie in Schritt 6 erläutert.

Traffic an eine EC2 Amazon-Instance weiterleiten

Amazon EC2 bietet skalierbare Rechenkapazität in der AWS Cloud. Sie können eine EC2 virtuelle Computerumgebung (eine Instance) mit einer vorkonfigurierten Vorlage (einem Amazon Machine Image oder AMI) starten. Wenn Sie eine EC2 Instance starten, EC2 werden das Betriebssystem (Linux oder Microsoft Windows) und zusätzliche im AMI enthaltene Software, wie Webserver- oder Datenbanksoftware, automatisch installiert.

Sie können Traffic für Ihre Domain, wie z. B. example.com, mithilfe von Amazon Route 53 auf Ihren Server weiterleiten, wenn Sie eine Website hosten oder eine Webanwendung auf einer EC2 Instance ausführen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Eine EC2 Amazon-Instanz. Informationen zum Starten einer EC2 Instance finden Sie in der folgenden Dokumentation:
  - Linux — Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 Linux-Instances im EC2 Amazon-Benutzerhandbuch
  - Microsoft Windows — Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 Windows-Instances im EC2 Amazon-Benutzerhandbuch

  > **Important**
  >
  > Wir empfehlen, dass Sie auch eine Elastic IP-Adresse erstellen und diese Ihrer EC2 Instance zuordnen. Eine Elastic IP-Adresse stellt sicher, dass sich die IP-Adresse Ihrer EC2 Amazon-Instance niemals ändert. Informationen zu den Preisen finden Sie unter Preise für Elastic-IP-Adressen.

- Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.

- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter für Ihre Domain finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an eine EC2 Amazon-Instance

Gehen Sie wie folgt vor, um Amazon Route 53 so zu konfigurieren, dass der Datenverkehr an eine EC2 Instance weitergeleitet wird.

Um Traffic an eine EC2 Amazon-Instance weiterzuleiten

1. Rufen Sie die IP-Adresse für die EC2 Amazon-Instance ab:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

   b. Wählen Sie in der Liste der Regionen in der rechten oberen Ecke der Konsole die Region aus, in der Sie die Instance gestartet haben.

   c. Wählen Sie im Navigationsbereich Instances aus.

   d. Wählen Sie in der Tabelle den Namen der Instance aus, an die Sie den Datenverkehr leiten möchten.

   e. Rufen Sie im unteren Bereich auf der Registerkarte Beschreibung den Wert von Elastic ab IPs.

      Wenn Sie der Instance keine Elastic IP-Adresse zugeordnet haben, rufen Sie den Wert von IPv4 Public IP ab.

2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie den Namen der gehosteten Zone für den Namen der Domain, für die Sie Datenverkehr weiterleiten wollen.
5. Wählen Sie Datensatz erstellen.
6. Geben Sie die folgenden Werte an:

Routing-Richtlinie

Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Traffic an Ihre EC2 Instance weiterzuleiten. Der Standardwert ist der Name der gehosteten Zone.

Wenn der Name der gehosteten Zone beispielsweise example.com lautet und Sie acme.example.com verwenden möchten, um Traffic an Ihre EC2 Instance weiterzuleiten, geben Sie acme ein.

Bewerten/Weiterleiten des Datenverkehrs an

Klicken Sie auf IP-Adresse oder ein anderer Wert, abhängig vom Datensatztyp. Geben Sie die IP-Adresse ein, die Sie in Schritt 1 erhalten haben.

Datensatztyp

Wählen IPv4 Sie A — Adresse.

TTL (Sekunden)

Übernehmen Sie den Standardwert 300.

7. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Weitergabe abgeschlossen ist, können Sie den Datenverkehr an Ihre EC2 Instance weiterleiten, indem Sie den Namen des Datensatzes verwenden, den Sie in diesem Verfahren erstellt haben.

> **Important**
>
> Achten Sie beim Freigeben der Elastic IP darauf, dass Sie auch den DNS-Datensatz löschen, der darauf verweist. Andernfalls haben Sie einen hängenden DNS-Datensatz, der von einem nicht autorisierten Benutzer übernommen werden kann.

Weiterleiten des Datenverkehrs an einen AWS App Runner Dienst

AWS App Runner ist ein vollständig verwalteter Service, der es Entwicklern leicht macht, containerisierte Webanwendungen APIs in großem Umfang bereitzustellen, ohne dass vorherige Infrastrukturkenntnisse erforderlich sind. Beginnen Sie mit Ihrem Quellcode oder einem Container-Image. App Runner erstellt und stellt die Webanwendung automatisch bereit, gleicht den Datenverkehr mit der Verschlüsselung aus, skaliert, um Ihren Datenverkehrsanforderungen gerecht zu werden, und erleichtert es Ihren Services, mit anderen AWS Services und Anwendungen zu kommunizieren, die in einer privaten Amazon VPC ausgeführt werden. Mit App Runner haben Sie mehr Zeit, sich auf Ihre Anwendungen zu konzentrieren, anstatt über Server oder Skalierung nachzudenken. Weitere Informationen finden Sie unter Was ist AWS App Runner im AWS App Runner -Entwicklerhandbuch.

> **Important**
>
> Amazon Route 53 unterstützt derzeit Aliaseinträge für AWS App Runner Services, die nach dem 1. August 2022 erstellt wurden.

Um den Datenverkehr der Domain an einen App-Runner-Dienst weiterzuleiten, erstellen Sie mithilfe von Amazon Route 53 einen Aliasdatensatz, der auf den App-Runner-Dienst verweist. Ein Alias-Datensatz ist eine Route-53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomain, z. B. example.com, als auch für Subdomains, z. B. www.example.com (http://www.example.com) verwenden. Sie können nur CNAME-Datensätze für Subdomains erstellen.

> **Note**
>
> Route 53 berechnet keine Gebühren für Alias-Abfragen an App-Runner-Dienste oder andere AWS -Ressourcen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Einen App-Runner-Dienst. Hinweise zum Erstellen eines App Runner-Dienstes finden Sie unter Erste Schritte mit App Runner.

- Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter für Ihre Domain finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.
- Hat die benutzerdefinierte Domain mit Ihrem App-Runner-Dienst verknüpft. Weitere Informationen finden Sie unter Verwalten benutzerdefinierter Domainnamen für App Runner.
- Konfigurieren Sie den Zertifikatsüberprüfungsdatensatz, der von App Runner an Ihre von Route 53 gehostete Zone zurückgegeben wird, um den Domainvalidierungsprozess zu starten. Weitere Informationen finden Sie unter DNS-Validierung im AWS Certificate Manager im AWS Certificate Manager -Benutzerhandbuch.

Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen App-Runner-Dienst

Zum Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen App-Runner-Dienst führen Sie die folgenden Schritte aus:

Weiterleiten des Datenverkehrs an einen App-Runner-Dienst

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den Namen der gehosteten Zone für den Namen der Domain, für die Sie Datenverkehr weiterleiten wollen.
4. Wählen Sie Datensatz erstellen.
5. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an den App-Runner-Dienst zu leiten. Der Standardwert ist der Name der gehosteten Zone.

Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihren App-Runner-Dienst zu leiten, geben Sie acme ein.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias für App-Runner-Dienst und wählen Sie dann die AWS-Region. Wählen Sie den Domainnamen der Umgebung aus, an die Sie den Datenverkehr weiterleiten möchten.

Datensatztyp

Akzeptieren Sie den Standardwert A — IPv4 Adresse.

Evaluate Target Health

Wählen Sie Nein. Informationen zur Bewertung des Zielzustands finden Sie unterEvaluate Target Health.

6. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an den App-Runner-Dienst leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleiten des Datenverkehrs zu einem AWS Global Accelerator

AWS Global Accelerator ist ein Dienst, in dem Sie Beschleuniger erstellen, um die Leistung Ihrer Anwendungen für lokale und globale Benutzer zu verbessern. Der Dienst reagiert sofort auf Änderungen des Zustands oder der Konfiguration, um sicherzustellen, dass der Internetverkehr von Clients immer an fehlerfreie Endgeräte geleitet wird. Global Accelerator verfügt über eine fehlertolerante Architektur und bietet AWS Shield Standard eine automatische Inline-Abwehr gegen S-Angriffe. DDo Weitere Informationen finden Sie im AWS Global Accelerator Entwicklerhandbuch unter Was ist Global Accelerator.

Standardmäßig stellt Ihnen Global Accelerator statische IP-Adressen zur Verfügung, die Sie Ihrem Accelerator zuordnen. Die statischen IP-Adressen stammen per Anycast aus dem AWS

Edge-Netzwerk. Accelerators enthalten einen Standard-DNS-Namen, aber in den meisten Szenarien können Sie DNS so konfigurieren, dass Ihr benutzerdefinierter Domainname (z. B. www.example.com) mit Ihrem Accelerator verwendet wird, anstatt die zugewiesenen statischen IP-Adressen oder den Standard-DNS-Namen zu verwenden.

> **Note**
>
> Route 53 erhebt keine Gebühren für Aliasabfragen an Global Accelerator oder andere Ressourcen. AWS

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Ein Beschleuniger. Sie können entweder einen Standardbeschleuniger oder einen benutzerdefinierten Routing-Beschleuniger erstellen. Weitere Informationen finden Sie unter Erstellen eines Standardbeschleunigers und Erstellen eines benutzerdefinierten Routingbeschleunigers.
- Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter für Ihre Domain finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfiguration von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen Accelerator

Gehen Sie wie folgt vor, um Amazon Route 53 so zu konfigurieren, dass der Verkehr an einen Accelerator weitergeleitet wird.

Um den Verkehr an einen Accelerator weiterzuleiten

1. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

3. Wählen Sie den Namen der gehosteten Zone für den Namen der Domain, für die Sie Datenverkehr weiterleiten wollen.
4. Wählen Sie Datensatz erstellen.
5. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

   Datensatzname

   Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an Ihren Accelerator weiterzuleiten. Der Standardwert ist der Name der gehosteten Zone.

   Wenn der Name der gehosteten Zone beispielsweise example.com lautet und Sie acme.example.com verwenden möchten, um Traffic an Ihren Global Accelerator weiterzuleiten, geben Sie acme ein.

   Bewerten/Weiterleiten des Datenverkehrs an

   Wählen Sie Alias to Global Accelerator und wählen Sie dann die. AWS-Region Wählen Sie den DNS-Namen für den Accelerator.

   Sie können den DNS-Namen eines Accelerators eingeben, den Sie mit dem aktuellen AWS-Konto oder einem anderen Accelerator erstellt haben AWS-Konto.

   Datensatztyp

   Akzeptieren Sie den Standardwert A — IPv4 Adresse.

   Evaluate Target Health

   Übernehmen Sie den Standardwert Ja.
6. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Weitergabe abgeschlossen ist, können Sie den Datenverkehr an Ihren Accelerator weiterleiten, indem Sie den Namen des Alias-Datensatzes verwenden, den Sie in diesem Verfahren erstellt haben.

Weiterleiten des Datenverkehrs an eine AWS Elastic Beanstalk Umgebung

Wenn Sie Anwendungen in der AWS Cloud bereitstellen und verwalten, können Sie Amazon Route 53 verwenden, um den DNS-Verkehr für Ihre Domain, z. B. example.com, an eine neue oder eine bestehende Elastic Beanstalk-Umgebung weiterzuleiten. AWS Elastic Beanstalk

Hinweise zum Weiterleiten von DNS-Datenverkehr an eine Elastic-Beanstalk-Umgebung finden Sie in den folgenden Themen.

> **Note**
>
> In diesen Verfahren wird davon ausgegangen, dass Sie bereits Route 53 als DNS-Service für Ihre Domain nutzen. Wenn Sie einen anderen DNS-Service verwenden, finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen weitere Informationen über die Verwendung von Route 53 als DNS-Dienstanbieter für Ihre Domain.

Themen

Bereitstellen einer Anwendung in einer Elastic-Beanstalk-Umgebung

Wenn Sie bereits über eine Elastic-Beanstalk-Umgebung verfügen, an die Sie Datenverkehr weiterleiten möchten, fahren Sie mit Abrufen des Domainnamens für die Elastic-Beanstalk-Umgebung fort.

So erstellen Sie eine Anwendung und stellen sie in einer Elastic-Beanstalk-Umgebung bereit

- Informationen zum Erstellen einer Anwendung und deren Bereitstellung in einer Elastic-Beanstalk-Umgebung finden Sie unter Erste Schritte mit Elastic Beanstalk im AWS Elastic Beanstalk - Entwicklerhandbuch.

Abrufen des Domainnamens für die Elastic-Beanstalk-Umgebung

Wenn Sie den Domainnamen für Ihre Elastic Beanstalk-Umgebung bereits kennen, fahren Sie mit Erstellen eines Amazon-Route-53-Datensatzes, der den Datenverkehr an Ihre Elastic-Beanstalk-Umgebung weiterleitet fort.

Abrufen des Domainnamens für die Elastic-Beanstalk-Umgebung

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Elastic Beanstalk Beanstalk-Konsole unter. https://console.aws.amazon.com/elasticbeanstalk/
2. Suchen Sie in der Liste der Anwendungen die Anwendung, an die Sie den Datenverkehr weiterleiten möchten, und rufen Sie den Wert für URL ab. Falls Sie keine Liste der Anwendungen sehen, wählen Sie im Navigationsbereich Applications (Anwendungen) aus.

   Weitere Informationen zur URL finden Sie unter Domainname der Elastic Beanstalk-Umgebung im Elastic Beanstalk Entwicklerleitfaden.

Erstellen eines Amazon-Route-53-Datensatzes, der den Datenverkehr an Ihre Elastic-Beanstalk-Umgebung weiterleitet

Ein Amazon-Route-53-Datensatz enthält die Einstellungen, die steuern, wie der Datenverkehr in Ihre Elastic-Beanstalk-Umgebung weitergeleitet wird. Sie erstellen entweder einen CNAME-Datensatz oder einen Alias-Datensatz, je nachdem, ob der Domainname für die Umgebung die Region (z. B. us-east-2) enthält, in der Sie die Umgebung bereitgestellt haben. Neue Umgebungen enthalten die Region im Domainnamen; Umgebungen, die vor Anfang 2016 erstellt wurden, nicht. Einen Vergleich der CNAME- und Alias-Datensätze finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Wenn der Domainname nicht die Region enthält

Sie müssen einen CNAME-Datensatz erstellen. Aufgrund der durch DNS bedingten Einschränkungen können Sie CNAME-Datensätze jedoch nur für Subdomains erstellen, nicht für den Root-Domainnamen. Wenn der Domainname beispielsweise example.com ist, können Sie einen Datensatz erstellen, der den Datenverkehr für acme.example.com an Ihre Elastic Beanstalk-Umgebung leitet. Sie können jedoch keinen Datensatz erstellen, der den Datenverkehr für example.com an Ihre Elastic Beanstalk-Umgebung leitet.

Siehe Verfahren unter So erstellen Sie einen CNAME-Datensatz, um Datenverkehr an eine Elastic-Beanstalk-Umgebung zu leiten:.

Wenn der Domainname die Region enthält

Sie können einen Alias-Datensatz erstellen. Ein Alias-Datensatz gilt speziell für Route 53 und verfügt über zwei wesentliche Vorteile gegenüber CNAME-Datensätzen:

- Sie können Alias-Datensätze für den Stammdomainnamen oder für Subdomains erstellen. Wenn der Domainname beispielsweise example.com ist, können Sie einen Datensatz erstellen, der Anfragen für example.com oder für acme.example.com an Ihre Elastic-Beanstalk-Umgebung weiterleitet.
- Route 53 berechnet keine Gebühren für Anfragen, die einen Alias-Datensatz für die Weiterleitung des Datenverkehrs verwenden.

Siehe Verfahren unter So erstellen Sie einen Amazon-Route-53-Aliasdatensatz, um Datenverkehr an eine Elastic-Beanstalk-Umgebung weiterzuleiten.

So erstellen Sie einen CNAME-Datensatz, um Datenverkehr an eine Elastic-Beanstalk-Umgebung zu leiten:

1. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter. https://console.aws.amazon.com/route53/
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den Namen der gehosteten Zone für den Domainnamen aus, den Sie verwenden möchten, um den Datenverkehr an die Elastic-Beanstalk-Umgebung zu leiten.
4. Wählen Sie Datensatz erstellen.
5. Wählen Sie Zur Schnellerstellung wechseln
6. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

   Datensatzname

   Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an eine Elastic Beanstalk-Umgebung zu leiten. Der Standardwert ist der Name der gehosteten Zone.

Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihre Umgebung zu leiten, geben Sie acme ein.

> **Important**
>
> Es ist nicht möglich, einen CNAME-Datensatz zu erstellen, der denselben Namen wie die gehostete Zone hat.

Alias

Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie je nach Datensatztyp IP-Adresse oder einen anderen Wert und geben Sie den Wert ein, den Sie erhalten, wenn Sie das Verfahren im Thema Abrufen des Domainnamens für die Elastic-Beanstalk-Umgebung ausführen. Wenn Sie zum Erstellen Ihrer Route-53-gehosteten Zone und Ihrer Elastic-Beanstalk-Umgebung unterschiedliche Konten verwendet haben, geben Sie die CNAME-Attribute für die Elastic-Beanstalk-Umgebung ein.

Datensatztyp

Klicken Sie auf CNAME.

TTL (Sekunden)

Übernehmen Sie den Standardwert 300.

7. Wählen Sie Create records (Datensätze erstellen).

   Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen.

So erstellen Sie einen Amazon-Route-53-Aliasdatensatz, um Datenverkehr an eine Elastic-Beanstalk-Umgebung weiterzuleiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

3. Wählen Sie den Namen der gehosteten Zone für den Domainnamen aus, den Sie verwenden möchten, um den Datenverkehr an die Elastic-Beanstalk-Umgebung zu leiten.
4. Wählen Sie Datensatz erstellen.
5. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

   Datensatzname

   Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an eine Elastic Beanstalk-Umgebung zu leiten. Der Standardwert ist der Name der gehosteten Zone.

   Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihre Umgebung zu leiten, geben Sie acme ein.

   Bewerten/Weiterleiten des Datenverkehrs an

   Wählen Sie Alias zu Elastic-Beanstalk-Umgebung und dann die Region aus, aus der der Endpunkt stammt. Wählen Sie den Domainnamen der Umgebung aus, an die Sie den Datenverkehr weiterleiten möchten. Dies ist der Wert, den Sie erhalten, wenn Sie das Verfahren im Thema Abrufen des Domainnamens für die Elastic-Beanstalk-Umgebung durchführen.

   Wenn Sie zum Erstellen Ihrer Route-53-gehosteten Zone und Ihrer Elastic-Beanstalk-Umgebung unterschiedliche Konten verwendet haben, geben Sie die CNAME-Attribute für die Elastic-Beanstalk-Umgebung ein.

   Datensatztyp

   Akzeptieren Sie die IPv4 Standardadresse A —.

   Evaluate Target Health

   Übernehmen Sie den Standardwert Ja.
6. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an die Elastic-Beanstalk-Umgebung leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellen.

Weiterleiten von Datenverkehr an einen ELB Load Balancer

Wenn Sie eine Website auf mehreren EC2 Amazon-Instances hosten, können Sie den Traffic auf Ihre Website mithilfe eines Elastic Load Balancing (ELB) -Load Balancers auf die Instances verteilen. Der ELB-Service skaliert automatisch den Load Balancer, wenn sich der Datenverkehr der Website im Laufe der Zeit ändert. Der Load Balancer überwacht auch den Zustand seiner registrierten Instances und leitet den Datenverkehr nur an ordnungsgemäß funktionierende Instances weiter.

Um Domaindatenverkehr an einen ELB-Load-Balancer weiterzuleiten, verwenden Sie Amazon Route 53, um einen Aliasdatensatz zu erstellen, der auf Ihren Load Balancer verweist. Ein Alias-Datensatz ist eine Route-53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomain (z. B. example.com) als auch für Subdomains (z. B. www.example.com) verwenden. (Sie können CNAME-Datensätze nur für Subdomains erstellen.)

> **Note**
>
> Route 53 berechnet keine Gebühren für Alias-Abfragen an ELB-Load-Balancer oder andere AWS -Ressourcen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Einen ELB Load Balancer. Sie können einen ELB Classic, Application oder Network Load Balancer verwenden. Informationen zum Erstellen eines Load Balancers finden Sie unter Erste Schritte mit Elastic Load Balancing im Elastic-Load-Balancing-Benutzerhandbuch.

  Geben Sie dem Load Balancer einen Namen, an den Sie sich zu einem späteren Zeitpunkt noch erinnern. Der Name, den Sie angeben, wenn Sie einen Load Balancer erstellen, ist der Name, den Sie auswählen, wenn Sie einen Alias-Datensatz in der Route-53-Konsole erstellen.

- Einen registrierten Domainnamen. Sie können Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen ELB Load Balancer

Zum Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen ELB Load Balancer führen Sie die folgenden Schritte aus.

So leiten Sie Datenverkehr an einen ELB Load Balancer

1. Wenn Sie die gehostete Route-53-Zone und den ELB Load Balancer mit demselben Konto erstellt haben, gehen Sie direkt weiter zu Schritt 2.

   Wenn Sie die gehostete Zone und den ELB Load Balancer mit verschiedenen Konten erstellt haben, führen Sie die Prozedur Abrufen des DNS-Namens für einen Elastic Load Balancing Load Balancer aus, um den DNS-Namen für den Load Balancer zu erhalten.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie den Namen der gehosteten Zone mit dem Domainnamen aus, den Sie verwenden möchten, um den Datenverkehr an den Load Balancer zu leiten.
5. Wählen Sie Datensatz erstellen.
6. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an den ELB Load Balancer zu leiten. Der Standardwert ist der Name der gehosteten Zone.

Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihren Load Balancer zu leiten, geben Sie acme ein.

Alias

Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias zu Application und Classic Load Balancer oder Alias zu Network Load Balancer und dann die Region aus, aus der der Endpunkt stammt.

Wenn Sie die gehostete Zone und den ELB-Load Balancer mit demselben AWS Konto erstellt haben, wählen Sie den DNS-Namen, den Sie dem Load Balancer bei der Erstellung zugewiesen haben.

Wenn Sie die gehostete Zone und den ELB-Load Balancer mit verschiedenen Konten erstellt haben, geben Sie den Wert ein, den Sie in Schritt 1 dieser Prozedur erhalten haben.

> **Note**
>
> Die Konsole stellt Dualstack voran. nur auf den DNS-Namen der Anwendung und des Classic Load Balancer von demselben AWS Konto aus. Wenn ein Client, z. B. ein Webbrowser, die IP-Adresse für Ihren Domainnamen (example.com) oder Ihren Subdomainnamen (www.example.com) anfordert, kann der Client eine Adresse (einen A-Record), eine IPv4 Adresse (einen AAAA-Record) oder beides IPv4 und IPv6 Adressen (in separaten Anfragen mit first) anfordern. IPv6 IPv4 Die Qualifizierung dualstack. ermöglicht Route 53, mit der jeweiligen IP-Adresse für Ihren Load Balancer zu antworten, abhängig vom IP-Adressenformat, das der Client angefordert hat. Sie müssen dualstack. für Application und Classic Load Balancer aus dem anderen Konto voranstellen.

Datensatztyp

Wählen Sie A — Adresse. IPv4

Evaluate Target Health

Wenn Sie möchten, dass der Datenverkehr auf der Grundlage des Zustands Ihrer Ressourcen an Route 53 geleitet wird, wählen Sie Yes (Ja). Weitere Informationen über Zustandsprüfungen für Ihre Ressourcen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

7. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an den Load Balancer leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleiten von Datenverkehr an eine Website, die in einem Amazon-S3-Bucket gehostet wird.

Dieses Thema enthält umfassende Verfahren für die Weiterleitung von DNS-Verkehr an jeden Amazon Simple Storage Service-Bucket, der für statisches Website-Hosting konfiguriert ist. Wenn Sie eine statische Website mit Amazon Simple Storage Service einrichten, finden Sie Verwenden Sie Ihre Domain für eine statische Website in einem Amazon S3 Bucket ein vollständiges Tutorial unter.

Amazon Simple Storage Service (Amazon S3) stellt sicheren, dauerhaften und hochskalierbaren Cloudspeicher bereit. Sie können einen S3-Bucket konfigurieren, um eine statische Website zu hosten, wie z. B. Webseiten und clientseitige Skripts. (S3 unterstützt kein serverseitiges Skripting.)

Um den Datenverkehr der Domain an einen S3 Bucket weiterzuleiten, erstellen Sie mithilfe von Amazon Route 53 einen Aliasdatensatz, der auf den Bucket verweist. Ein Alias-Datensatz ist eine Route-53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomain (z. B. example.com) als auch für Subdomains (z. B. www.example.com) verwenden. Sie können CNAME-Datensätze nur für Subdomains erstellen.

> **Note**
>
> Route 53 berechnet keine Gebühren für Alias-Abfragen an S3 Buckets oder andere AWS -Ressourcen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Ein S3-Bucket, der zum Hosten einer statischen Website konfiguriert ist.

  Weitere Informationen finden Sie unter Tutorial: Konfiguration einer statischen Website mithilfe einer benutzerdefinierten Domain, die bei Route 53 registriert ist, im Amazon Simple Storage Service-Benutzerhandbuch.

  > **Important**
  >
  > Der Bucket muss denselben Namen haben wie die Domain oder Subdomain. Wenn Sie beispielsweise die Subdomain acme.example.com verwenden wollen, muss der Bucket ebenfalls den Namen acme.example.com tragen.

  Sie können den Datenverkehr für eine Domain und deren Subdomain, wie z. B. example.com und www.example.com, in einen einzelnen Bucket weiterleiten. Erstellen Sie einen Bucket für die Domain und die einzelnen Subdomains, und konfigurieren Sie alle außer einem Bucket, um den Datenverkehr auf den verbleibenden Bucket umzuleiten.

  > **Note**
  >
  > Ein S3-Bucket, der als Website-Endpunkt konfiguriert ist, unterstützt SSL/TLS nicht. Sie müssen also den Datenverkehr an die CloudFront Distribution weiterleiten und den S3-Bucket als Ursprung für die Verteilung verwenden.
  > Anweisungen zum Erstellen einer CloudFront Distribution finden Sie unter. Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens

- Einen registrierten Domainnamen. Sie können Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.

- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

  Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen S3 Bucket

Um Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen S3 Bucket zu konfigurieren, der eine statische Website hostet, führen Sie die folgenden Schritte durch.

So leiten Sie den Datenverkehr an einen S3-Bucket

1. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie den Namen der gehosteten Zone mit dem Domainnamen aus, den Sie verwenden möchten, um den Datenverkehr an den S3-Bucket zu leiten.
4. Wählen Sie Datensatz erstellen.
5. Geben Sie die folgenden Werte an:

   Datensatzname

   Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an den S3-Bucket zu leiten. Der Standardwert ist der Name der gehosteten Zone.

   Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihren Bucket zu leiten, geben Sie acme ein.

   Datensatztyp

   Wählen Sie A — IPv4 Adresse.

   Alias

   Schalten Sie Alias ein.

Datenverkehr weiterleiten an

Wählen Sie Alias zu S3-Website-Endpunkt und dann die Region aus, aus der der Endpunkt stammt.

Wählen Sie den Bucket mit demselben Namen aus, den Sie für Datensatzname angegeben haben.

Die Liste enthält nur dann einen Bucket, wenn der Bucket die folgenden Anforderungen erfüllt:

- Der Name des Buckets stimmt mit dem Namen des Datensatzes überein, den Sie anlegen.
- Der Bucket ist als Website-Endpunkt konfiguriert.
- Der Bucket wurde durch das aktuelle AWS -Konto erstellt.

  Wenn Sie den Bucket mithilfe eines anderen AWS -Kontos erstellt haben, geben Sie den Namen der Region ein, in der Sie Ihren S3-Bucket erstellt haben. Das richtige Format für den Regionsnamen finden Sie in der Spalte Website-Endpunkt in der Tabelle Amazon-S3-Website-Endpunkte im Allgemeine Amazon Web Services-Referenz.

Evaluate Target Health

Wählen Sie Nein. Informationen zur Bewertung des Zielzustands finden Sie unterEvaluate Target Health.

Routing-Richtlinie

Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

6. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an den S3-Bucket leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleiten des Datenverkehrs an einen Amazon-Virtual-Private Cloud-Schnittstellenendpunkt unter Verwendung Ihres Domainnamens

Sie können verwenden AWS PrivateLink , um mit einem Amazon Virtual Private Cloud (Amazon VPC) -Schnittstellenendpunkt auf ausgewählte Services zuzugreifen. Zu diesen Services gehören einige AWS Services, Services, die von anderen AWS Kunden und Partnern eigenständig gehostet werden VPCs, sowie unterstützte AWS Marketplace Partnerservices.

Um den Domainverkehr an einen Schnittstellenendpunkt weiterzuleiten, verwenden Sie Amazon Route 53 zur Erstellung eines Aliasdatensatzes. Ein Alias-Datensatz ist eine Route-53-Erweiterung von DNS. Er funktioniert ähnlich wie ein CNAME-Datensatz, jedoch können Sie einen Alias-Datensatz sowohl für die Stammdomain (z. B. example.com) als auch für Subdomains (z. B. www.example.com) verwenden. Sie können CNAME-Datensätze nur für Subdomains erstellen.

> **Note**
>
> Route 53 erhebt keine Gebühren für Aliasabfragen an Schnittstellenendpunkte oder andere AWS Ressourcen.

Themen

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Amazon-VPC-Schnittstellenendpunkt. Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.
- Einen registrierten Domainnamen. Sie können Amazon Route 53 als Domainvergabestelle verwenden oder eine andere Vergabestelle nutzen.
- Route 53 als DNS-Service für die Domain. Wenn Sie mithilfe von Route 53 Ihren Domainnamen registrieren, konfigurieren wir automatisch Route 53 als DNS-Service für die Domain.

Weitere Informationen zur Verwendung von Route 53 als DNS-Serviceanbieter finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfigurieren von Amazon Route 53 zum Weiterleiten von Datenverkehr an einen Endpunkt der Amazon-VPC-Schnittstelle

Zum Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an einen Amazon-VPC-Schnittstellenendpunkt führen Sie die folgenden Schritte aus.

So leiten Sie den Datenverkehr zu einem Amazon VPC-Schnittstellenendpunkt weiter

1. Wenn Sie die gehostete Route-53-Zone und den Amazon-VPC-Schnittstellenendpunkt mit demselben Konto erstellt haben, fahren Sie mit Schritt 2 fort.

   Wenn Sie die gehostete Zone und den Schnittstellenendpunkt mit verschiedenen Konten erstellt haben, rufen Sie den Servicenamen für den Schnittstellenendpunkt ab:

   a. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
   b. Wählen Sie im Navigationsbereich Endpunkte aus.
   c. Wählen Sie im rechten Bereich den Endpunkt, zu dem Sie den Internetverkehr weiterleiten möchten.
   d. Rufen Sie im unteren Bereich den Wert des DNS-Namens ab, z. B. vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com.
2. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie den Namen der gehosteten Zone mit dem Domainnamen aus, den Sie verwenden möchten, um den Datenverkehr an den Schnittstellenendpunkt zu leiten.
5. Wählen Sie Datensatz erstellen.
6. Geben Sie die folgenden Werte an:

   Routing-Richtlinie

   Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

Datensatzname

Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an den Amazon-VPC-Schnittstellenendpunkt zu leiten.

Alias

Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias zu VPC-Endpunkt und dann die Region aus, aus der der Endpunkt stammt.

Wie Sie den Wert für Endpoints angeben, hängt davon ab, ob Sie die Hosting-Zone und den Schnittstellenendpunkt mit demselben AWS Konto oder mit unterschiedlichen Konten erstellt haben:

- Gleiches Konto – Wählen Sie die Liste aus und suchen Sie die Kategorie Amazon-VPC-Endpunkte. Wählen Sie dann den DNS-Namen des Schnittstellenendpunkts, an den Sie den Internetverkehr weiterleiten möchten.
- Unterschiedliche Konten – Geben Sie den Wert ein, den Sie in Schritt 1 dieser Vorgehensweise erhalten haben.

Datensatztyp

Wählen Sie A — IPv4 Adresse.

Evaluate Target Health

Wählen Sie Nein. Informationen zur Bewertung des Zielzustands finden Sie unterEvaluate Target Health.

7. Wählen Sie Create records (Datensätze erstellen).

Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Übertragung abgeschlossen ist, können Sie den Datenverkehr an den Schnittstellenendpunkt leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleitung des Datenverkehrs an Amazon WorkMail

Sie können Route 53 verwenden, um den Verkehr an Ihre WorkMail Amazon-E-Mail-Domain weiterzuleiten. Der Name Ihrer von Route 53 gehosteten Zone (z. B. example.com) muss mit dem Namen einer WorkMail Amazon-Domain übereinstimmen.

> **Note**
>
> Sie können Traffic nur für öffentlich gehostete Zonen an eine WorkMail Amazon-Domain weiterleiten.

Um den Verkehr an Amazon weiterzuleiten WorkMail, führen Sie die folgenden vier Verfahren durch.

Um Amazon Route 53 als Ihren DNS-Service zu konfigurieren und eine WorkMail Amazon-Organisation und eine E-Mail-Domain hinzuzufügen

1. Wenn Sie den Domainnamen, den Sie in Ihren E-Mail-Adressen verwenden möchten (z. B. john@example.com), noch nicht registriert haben, registrieren Sie die Domain jetzt, damit Sie wissen, ob die Domain verfügbar ist. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

   Wenn Amazon Route 53 nicht der DNS-Service für die E-Mail-Domain ist, die Sie zu Amazon hinzugefügt haben WorkMail, migrieren Sie den DNS-Service für die Domain zu Route 53. Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.
2. Fügen Sie eine WorkMail Amazon-Organisation und eine E-Mail-Domain hinzu. Weitere Informationen finden Sie unter Erste Schritte für neue Benutzer im WorkMail Amazon-Administratorhandbuch.

So erstellen Sie einen Route 53-TXT-Datensatz für Amazon WorkMail

1. Wählen Sie im Navigationsbereich der WorkMail Amazon-Konsole Domains aus.
2. Wählen Sie den Namen der E-Mail-Domain, z. B. example.com, die Sie verwenden möchten, um den Traffic an Amazon WorkMail weiterzuleiten.
3. Öffnen Sie eine weitere Browser-Registerkarte, und öffnen Sie die Route-53-Konsole.
4. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

a. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
b. Wählen Sie den Namen der gehosteten Zone, die Sie für Ihre WorkMail Amazon-E-Mail-Domain verwenden möchten.

5. Gehen Sie in der WorkMail Amazon-Konsole im Abschnitt Schritt 1: Domain-Inhaberschaft verifizieren zur Spalte Hostname und kopieren Sie den Teil des Werts, der Ihrem E-Mail-Domainnamen vorausgeht.

   Wenn Ihre WorkMail Amazon-E-Mail-Domain beispielsweise example.com lautet und der Wert von Hostname _amazonses.example.com ist, kopieren Sie _amazonses.

6. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

   a. Klicken Sie auf Erstellen von Datensätzen und wählen Sie Einfaches Routing aus.
   b. Fügen Sie für Datensatzname den Wert ein, den Sie zuvor in Schritt 5 kopiert haben.
   c. Wählen Sie für den Record type (Datensatztyp) TXT – Text.

7. Kopieren Sie in der WorkMail Amazon-Konsole für den TXT-Eintrag den Wert der Spalte Value, einschließlich der Anführungszeichen.
8. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

   a. Wählen Sie für Wert/Route-Datenverkehr an je nach Datensatztyp IP-Adresse oder einen anderen Wert aus, und fügen Sie den in Schritt 7 kopierten Wert ein.

      Ändern Sie keine weiteren Einstellungen.
   b. Wählen Sie Erstellen aus.

So erstellen Sie einen Route 53-MX-Datensatz für Amazon WorkMail

1. Gehen Sie in der WorkMail Amazon-Konsole im Abschnitt Schritt 2: Domain-Setup abschließen zu der Zeile mit dem Record-Typ MX und kopieren Sie den Wert der Spalte Value.
2. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

   a. Wählen Sie Datensatz erstellen.
   b. Wählen Sie für Wert/Route-Datenverkehr an je nach Datensatztyp IP-Adresse oder einen anderen Wert aus, und fügen Sie den in Schritt 1 kopierten Wert ein.
   c. Wählen Sie als Datensatztyp MX – Mail Exchange.

      Ändern Sie keine weiteren Einstellungen.

d. Wählen Sie Create records (Datensätze erstellen).

So erstellen Sie vier Route 53-CNAME-Einträge für Amazon WorkMail

1. Gehen Sie in der WorkMail Amazon-Konsole im Abschnitt Schritt 2: Domain-Setup abschließen zur ersten Zeile, die den Record-Typ CNAME hat. Kopieren Sie in der Spalte Hostname den Teil des Werts vor Ihrem E-Mail-Domainnamen.

   Wenn Ihre WorkMail Amazon-E-Mail-Domain beispielsweise example.com lautet und der Wert von Hostname autodiscover.example.com lautet, kopieren Sie autodiscover.
2. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

   a. Wählen Sie Datensatz erstellen.
   b. Fügen Sie für Datensatzname den Wert ein, den Sie zuvor in Schritt 1 kopiert haben.
   c. Wählen Sie für Datensatztyp die Option CNAME - Canonical Name (CNAME – Kanonischer Name) aus.
3. Kopieren Sie in der WorkMail Amazon-Konsole in die erste Zeile, die den Record-Typ CNAME hat, den Wert der Spalte Value.
4. Führen Sie in der Route-53-Konsole die folgenden Schritte aus:

   a. Wählen Sie für Wert/Route-Datenverkehr an je nach Datensatztyp IP-Adresse oder einen anderen Wert aus, und fügen Sie den in Schritt 3 kopierten Wert ein.

      Ändern Sie keine weiteren Einstellungen.
   b. Wählen Sie Create records (Datensätze erstellen).
5. Wiederholen Sie die Schritte 1 bis 4 für die verbleibenden CNAME-Einträge, die in der WorkMail Amazon-Konsole aufgeführt sind.

Weiterleitung des Datenverkehrs an den Amazon OpenSearch Service-Domänenendpunkt

Amazon OpenSearch Service ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Clustern in der erleichtert AWS Cloud. Eine OpenSearch Service Service-Domain ist gleichbedeutend mit einem OpenSearch Service-Cluster. Domains sind Cluster mit den Einstellungen, Instance-Typen, Instance-Anzahl und Speicherressourcen, die Sie

angeben. Weitere Informationen finden Sie unter Was ist Amazon OpenSearch Service im Amazon OpenSearch Service Developer Guide.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

Eine OpenSearch Service-Domain mit einem benutzerdefinierten Domainnamen, wie z. B. example.com, der dem Namen des Route 53-Eintrags entspricht, den Sie erstellen möchten.

Weitere Informationen finden Sie unter den folgenden Themen:

- Erste Schritte im Amazon OpenSearch Service Developer Guide.
- Erstellen eines benutzerdefinierten Endpunkts im Amazon OpenSearch Service Developer Guide.

Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an einen Amazon OpenSearch Service-Domain-Endpunkt

Um Route 53 zur Weiterleitung von Datenverkehr an OpenSearch Service zu verwenden, erhalten Sie zunächst den von OpenSearch Service bereitgestellten Domain-Endpunkt. Dieser Dual-Stack-Endpunkt wird nur bereitgestellt, wenn der benutzerdefinierte Endpunkt in einer OpenSearch Service-Domain mit Dual-Stack-Netzwerkmodus aktiviert ist. Weitere Informationen finden Sie unter Erstellen eines benutzerdefinierten Endpunkts im Amazon OpenSearch Service Developer Guide.

Um den Verkehr an einen OpenSearch Service-Endpunkt weiterzuleiten

1. Gehen Sie zu https://aws.amazon.comund wählen Sie In der Konsole anmelden aus.
2. Wählen Sie unter Analytics Amazon OpenSearch Service aus.
3. Wählen Sie unter Verwaltete Cluster die Option Domains aus.
4. Wählen Sie auf der Seite Domains den Namen der Domain aus, an die Sie den Traffic weiterleiten möchten.
5. Kopieren Sie auf der Domain-Detailseite den Wert für den Domain-Endpunkt v2 (Dual-Stack).
6. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
7. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
8. Wählen Sie den verknüpften Namen der gehosteten Zone für die Domain aus, die Sie verwenden möchten, um den Datenverkehr an Ihren OpenSearch Service-Endpunkt weiterzuleiten. Der

Domainname muss mit dem im OpenSearch Service definierten benutzerdefinierten Endpunkt übereinstimmen.

9. Wählen Sie Datensatz erstellen.

   Sie können den Assistenten verwenden, um die Datensätze zu erstellen, oder wählen Sie Wechseln zu Schnellerstellung.

10. Geben Sie die folgenden Werte an:

    Routing-Richtlinie

    Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

    Datensatzname

    Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an Ihren OpenSearch Service-Domänenendpunkt weiterzuleiten. Der Standardwert ist der Name der gehosteten Zone.

    Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihre Verteilung zu leiten, geben Sie acme ein.

    Alias

    Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

    Bewerten/Weiterleiten des Datenverkehrs an

    Wählen Sie Alias to OpenSearch Service Domain-Endpunkt aus. Wählen Sie die Region aus, in der die OpenSearch Service-Domain erstellt wurde, und wählen Sie den Wert aus, den Sie in Schritt 5 erhalten haben.

    Datensatztyp

    Wählen Sie IPv4 A-Adresse, IPv6 AAAA-Adresse oder beides für Dual-Stack.

    Evaluate Target Health

    Wählen Sie Nein. Informationen zur Bewertung des Zielzustands finden Sie unterEvaluate Target Health.

11. Wählen Sie Create records (Datensätze erstellen).

Weiterleiten des Datenverkehrs an den Domänenendpunkt des Amazon VPC Lattice-Dienstes

Amazon VPC Lattice ist ein vollständig verwalteter Anwendungsnetzwerkservice, mit dem Sie die Services und Ressourcen für Ihre Anwendung verbinden, sichern und überwachen. Sie können VPC Lattice mit einer einzelnen Virtual Private Cloud (VPC) oder über mehrere Konten VPCs hinweg verwenden. Weitere Informationen finden Sie unter Was ist Amazon VPC Lattice im Amazon VPC Lattice-Benutzerhandbuch.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

Eine VPC-Lattice-Dienstdomäne mit einem benutzerdefinierten Domänennamen, z. B. example.com, der dem Namen des Route 53-Datensatzes entspricht, den Sie erstellen möchten.

Weitere Informationen finden Sie unter Verknüpfen eines benutzerdefinierten Domainnamens mit Ihrem Service im Amazon VPC Lattice-Benutzerhandbuch.

Konfiguration von Amazon Route 53 zur Weiterleitung von Datenverkehr an einen VPC Lattice-Service-Domänenendpunkt

Um Route 53 zur Weiterleitung von Datenverkehr an die Amazon VPC Lattice-Service-Domain zu verwenden, rufen Sie zunächst den von VPC Lattice bereitgestellten Domain-Service-Endpunkt ab. Weitere Informationen finden Sie unter Verknüpfen eines benutzerdefinierten Domainnamens mit Ihrem Service im Amazon VPC Lattice-Benutzerhandbuch.

So leiten Sie den Datenverkehr an den Domänenendpunkt des VPC-Lattice-Dienstes weiter

1. Gehen Sie zu https://aws.amazon.comund wählen Sie In der Konsole anmelden aus.
2. Wählen Sie unter Networking & Content Delivery die Option VPC aus.
3. Wählen Sie unter PrivateLink und Lattice Lattice die Option Lattice Services aus.
4. Erstellen Sie einen VPC-Lattice-Dienst oder wählen Sie einen vorhandenen VPC-Lattice-Dienst aus.

> **Note**
>
> Wenn Sie einen VPC Lattice-Dienst erstellen, müssen Sie eine benutzerdefinierte Domänenkonfiguration und einen benutzerdefinierten Domänennamen angeben. Wenn Sie sich für einen vorhandenen Dienst entscheiden, muss dieser auch über eine benutzerdefinierte Domain verfügen.

5. Kopieren Sie unter Domänenkonfiguration den Wert für den benutzerdefinierten Domainnamen.
6. Öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
7. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
8. Wählen Sie den verknüpften Namen der gehosteten Zone für die Domain aus, die Sie verwenden möchten, um den Datenverkehr an Ihren VPC Lattice-Dienstdomänenendpunkt weiterzuleiten. Der Domainname muss mit dem in VPC Lattice definierten benutzerdefinierten Domänenendpunkt übereinstimmen.
9. Wählen Sie Datensatz erstellen.

   Sie können den Assistenten verwenden, um die Datensätze zu erstellen, oder wählen Sie Wechseln zu Schnellerstellung.
10. Geben Sie die folgenden Werte an:

    Routing-Richtlinie

    Wählen Sie die entsprechende Routing-Richtlinie. Weitere Informationen finden Sie unter Auswählen einer Routing-Richtlinie.

    Datensatzname

    Geben Sie den Domainnamen ein, den Sie verwenden möchten, um den Datenverkehr an Ihren VPC Lattice-Dienstdomänenendpunkt weiterzuleiten. Der Standardwert ist der Name der gehosteten Zone.

    Wenn der Name der gehosteten Zone beispielsweise "example.com" lautet und Sie acme.example.com verwenden möchten, um den Datenverkehr an Ihre Verteilung zu leiten, geben Sie acme ein.

    Alias

    Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias to VPC Lattice Service. Wählen Sie die Region aus, in der die VPC Lattice-Dienstdomäne erstellt wurde, und wählen Sie den Wert aus, den Sie in Schritt 5 erhalten haben.

Datensatztyp

Wählen Sie IPv4 A-Adresse, AAAA-Adresse oder beides für IPv6 Dual-Stack.

Evaluate Target Health

Wählen Sie Nein. Informationen zur Bewertung des Zielzustands finden Sie unterEvaluate Target Health.

11. Wählen Sie Create records (Datensätze erstellen).

Weiterleiten des Datenverkehrs an andere AWS Ressourcen

Es folgt eine Liste über Themen in anderen Leitfäden zur Verwendung von Route 53, um den Datenverkehr an diese Dienste weiterzuleiten.

- Benutzen von AWS Cloud Map im AWS Cloud Map -Benutzerhandbuch.
- Verwalten Sie benutzerdefinierte Domänen im AWS App Runner Developer Guide.
- Verwenden von Route 53 als DNS-Anbieter im AWS Transfer Family -Benutzerhandbuch.
- Verwenden von Route 53, um eine Domain auf eine Amazon-Lightsail-Instance zu verweisen.

Amazon Route 53-Zustandsprüfungen erstellen

Amazon Route 53-Zustandsprüfungen überwachen den Zustand und die Leistung Ihrer Webanwendungen, Webserver und anderer Ressourcen. Jede Zustandsprüfung, die Sie erstellen, kann eines der folgenden Elemente überwachen:

- Den Zustand einer bestimmten Ressource, z. B. eines Webservers
- Den Status anderer Zustandsprüfungen
- Der Status eines CloudWatch Amazon-Alarms.
- Darüber hinaus können Sie mit Amazon Application Recovery Controller (ARC) Zustandsprüfungen für die Routing-Kontrolle mit DNS-Failover-Einträgen einrichten, um den Datenverkehrs-Failover für Ihre Anwendung zu verwalten. Weitere Informationen finden Sie im Amazon Application Recovery Controller (ARC) Developer Guide.

Eine Übersicht über die drei Arten von Zustandsprüfungen finden Sie unter Arten von Amazon Route 53-Zustandsprüfungen. Weitere Informationen zum Erstellen von Zustandsprüfungen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Status der Zustandsprüfung sowie Benachrichtigungen über Statusänderungen erhalten und DNS Failover konfigurieren:

Den Status der Zustandsprüfung und Benachrichtigungen erhalten

Sie können den aktuellen und jüngsten Status Ihrer Zustandsprüfungen auf der Route 53-Konsole anzeigen. Sie können Integritätsprüfungen auch programmgesteuert über eine der APIs AWS SDKs, AWS Command Line Interface AWS Tools for Windows PowerShell, oder Route 53 durchführen.

Wenn Sie eine Benachrichtigung erhalten möchten, wenn sich der Status einer Gesundheitsprüfung ändert, können Sie für jede Zustandsprüfung einen CloudWatch Amazon-Alarm konfigurieren.

Weitere Informationen zum Anzeigen des Zustandsprüfungsstatus und Empfangen von Benachrichtigungen finden Sie unter Den Status von Zustandsprüfungen überwachen und Benachrichtigungen erhalten.

Konfigurieren von DNS Failover

Wenn Sie über mehrere Ressourcen verfügen, die dieselbe Funktion erfüllen, können Sie DNS Failover konfigurieren, damit Route 53 Ihren Datenverkehr von einer fehlerhaften Ressource an eine fehlerfreie Ressource leitet. Wenn Sie zum Beispiel über zwei Webserver verfügen und einer der Webserver fehlerhaft wird, kann Route 53 den Datenverkehr auf den anderen Webserver leiten. Weitere Informationen finden Sie unter Konfigurieren von DNS Failover.

Themen

Arten von Amazon Route 53-Zustandsprüfungen

Sie können die folgenden Arten von Amazon Route 53-Zustandsprüfungen erstellen:

Zustandsprüfungen, die einen Endpunkt überwachen

Sie können eine Zustandsprüfung für die Überwachung eines Endpunktes konfigurieren, den Sie entweder durch die IP-Adresse oder den Domänennamen festlegen. In regelmäßigen Intervallen, die Sie festlegen, sendet Route 53 automatisierte Anfragen über das Internet an Ihre Anwendung, den Server oder andere Ressourcen, um sicherzustellen, dass sie erreichbar, verfügbar und funktionsfähig sind. Optional können Sie die Zustandsprüfung so konfigurieren, dass sie ähnliche Anforderungen wie Ihre Benutzer vornimmt, also z. B. eine Website von einer bestimmten URL anfordert.

Zustandsprüfungen, die andere Zustandsprüfungen überwachen (berechnete Zustandsprüfungen)

Sie können eine Zustandsprüfung erstellen, die überwacht, ob Route 53 andere Zustandsprüfungen als fehlerfrei oder fehlerhaft ansieht. Dies kann nützlich sein, wenn Sie über mehrere Ressourcen verfügen, die dieselbe Funktion erfüllen, beispielsweise mehrere Webserver, und Ihre Hauptsorge darin besteht, ob eine bestimmte minimale Anzahl Ihrer

Ressourcen fehlerfrei ist. Sie können eine Zustandsprüfung für jede Ressource erstellen, ohne Benachrichtigungen für diese Zustandsprüfungen zu konfigurieren. Anschließend können Sie eine Zustandsprüfung erstellen, die den Status der anderen Zustandsprüfungen überwacht und Sie nur dann benachrichtigt, wenn die Anzahl der verfügbaren Webressourcen unter einen bestimmten Schwellenwert gesunken ist.

Gesundheitschecks zur Überwachung von CloudWatch Alarmen

Sie können CloudWatch Alarme erstellen, die den Status von CloudWatch Metriken überwachen, z. B. die Anzahl der gedrosselten Leseereignisse für eine Amazon DynamoDB DynamoDB-Datenbank oder die Anzahl der Elastic Load Balancing Balancing-Hosts, die als fehlerfrei gelten. Nachdem Sie einen Alarm erstellt haben, können Sie eine Integritätsprüfung durchführen, die denselben Datenstrom überwacht, der den Alarm CloudWatch überwacht.

Um die Resilienz und Verfügbarkeit zu verbessern, wartet Route 53 nicht darauf, dass der CloudWatch Alarm den `ALARM` Status erreicht. Der Status einer Integritätsprüfung ändert sich basierend auf dem Datenstrom und den Kriterien im Alarm von fehlerfrei zu fehlerhaft. CloudWatch

Route 53 unterstützt CloudWatch Alarme mit den folgenden Funktionen:

- Metriken mit Standardauflösung. Metriken mit hoher Auflösung werden nicht unterstützt. Weitere Informationen finden Sie unter Metriken mit hoher Auflösung im CloudWatch Amazon-Benutzerhandbuch.
- Statistiken: Durchschnitt, Minimum, Maximum, Summe und SampleCount. Erweiterte Statistiken werden nicht unterstützt.
- „M von N“ -Alarme werden von Route 53 nicht unterstützt. Weitere Informationen finden Sie im CloudWatch Amazon-Leitfaden unter Einen Alarm auswerten.
- Bei einem Gesundheitscheck kann nur ein CloudWatch Alarm überwacht werden, der sich auf demselben AWS Konto wie der Gesundheitscheck befindet.
- Route 53 unterstützt keine Alarme, die metrische Mathematik verwenden, um mehrere CloudWatch Messwerte abzufragen.

Routing-Controller für Amazon Application Recovery Controller (ARC)

Integritätsprüfungen in ARC sind mit Routingsteuerungen verknüpft, bei denen es sich um einfache Ein-/Ausschalter handelt. Sie konfigurieren jede Zustandsprüfung der Routingsteuerung mit einem Failover-DNS-Eintrag. Anschließend können Sie einfach Ihre Routing-Steuerungen in ARC aktualisieren, um den Datenverkehr umzuleiten und ein Failover für Ihre Anwendungen

durchzuführen, z. B. über Availability Zones oder AWS-Regionen hinweg. Weitere Informationen finden Sie unter Routing-Steuerung in ARC im ARC-Entwicklerhandbuch.

So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist

Die Methode, die Amazon Route 53 verwendet, um zu ermitteln, ob eine Zustandsprüfung fehlerfrei ist, hängt von der Art der Zustandsprüfung ab.

So ermittelt Route 53 den Status von Zustandsprüfungen zur Überwachung eines Endpunkts

Route 53 führt Zustandsprüfungen für Standorte auf der ganzen Welt durch. Wenn Sie eine Zustandsprüfung erstellen, die einen Endpunkt überwacht, sendet die Zustandsprüfung Anforderungen an den Endpunkt, den Sie angeben, um festzustellen, ob der Endpunkt störungsfrei arbeitet. Sie können die Standorte wählen, die Route 53 verwenden soll, und zudem das Prüfungsintervall festlegen: alle 10 Sekunden oder alle 30 Sekunden. Beachten Sie, dass Route 53-Zustandsprüfer in verschiedenen Rechenzentren nicht miteinander koordinieren, sodass Sie manchmal mehrere Anfragen pro Sekunde sehen, unabhängig des von Ihnen gewählten Intervalls, gefolgt von wenigen Sekunden ohne Zustandsprüfungen.

Jede Zustandsprüfung analysiert den Zustand eines Endpunkts anhand zweier Kriterien:

- Reaktionszeit. Bei einer Ressource reagiert der Service möglicherweise langsam oder antwortet nicht auf eine Anforderung für eine Statusprüfung aus einer Vielzahl von Gründen. Die Ressource ist beispielsweise wegen Wartungsarbeiten heruntergefahren, sie ist einem Distributed-Denial-of-Service (DDoS) -Angriff ausgesetzt oder das Netzwerk ist ausgefallen.
- Ob der Endpunkt auf eine Reihe aufeinander folgender von Ihnen angegebenen Zustandsprüfungen reagiert (der Fehlerschwellenwert)

Route 53 aggregiert die Daten der Zustandsprüfungen und bestimmt, ob ein Endpunkt fehlerfrei arbeitet.

- Wenn mehr als 18 % der Zustandsprüfungen ergeben, dass ein Endpunkt fehlerfrei arbeitet, gilt dieser für Route 53 als funktionsbereit.

- Wenn 18 % oder weniger der Zustandsprüfungen ergeben, dass ein Endpunkt fehlerfrei arbeitet, gilt dieser für Route 53 nicht als fehlerfrei.

Der Wert von 18 % wurde gewählt, um sicherzustellen, dass Zustandsprüfungen mehrerer Regionen den Endpunkt als störungsfrei bewerten. Dadurch wird verhindert, dass ein Endpunkt als nicht fehlerfrei gilt, nur weil der Endpunkt aufgrund von Netzwerkbedingungen von einigen zustandsprüfenden Standorten isoliert hat. Dieser Wert ändert sich möglicherweise in einer zukünftigen Version.

Die Reaktionszeit, die eine einzelne Zustandsprüfung nutzt, um zu ermitteln, ob ein Endpunkt fehlerfrei ist, hängt von der Art der Zustandsprüfung ab:

- HTTP- und HTTPS-Zustandsprüfungen - Route 53 muss innerhalb von vier Sekunden eine TCP-Verbindung mit dem Endpunkt herstellen können. Zusätzlich muss der Endpunkt innerhalb von zwei Sekunden nach dem Herstellen der Verbindung mit einem HTTP-Statuscode von 2xx oder 3xx reagieren.

  > **Note**
  >
  > HTTPS-Zustandsprüfungen validieren keine SSL/TLS Zertifikate, sodass Prüfungen nicht fehlschlagen, wenn ein Zertifikat ungültig oder abgelaufen ist.

- TCP-Zustandsprüfungen - Route 53 muss innerhalb von zehn Sekunden eine TCP-Verbindung mit dem Endpunkt herstellen können.
- HTTP- und HTTPS-Zustandsprüfungen mit Zeichenfolgenabgleich - Wie bei HTTP- und HTTPS-Zustandsprüfungen muss Route 53 innerhalb von vier Sekunden eine TCP-Verbindung mit dem Endpunkt herstellen können, und der Endpunkt muss innerhalb von zwei Sekunden nach dem Herstellen der Verbindung mit einem HTTP-Statuscode von 2xx oder 3xx reagieren.

  Nachdem ein Route 53-Zustandsprüfer den HTTP-Statuscode erhalten hat, muss er innerhalb der nächsten zwei Sekunden den Antworttext des Endpunkts erhalten. Route 53 durchsucht den Antworttext nach einer Zeichenfolge, die Sie angeben. Die Zeichenfolge muss vollständig in den ersten 5.120 Bytes des Antworttexts erscheinen oder der Endpunkt besteht die Zustandsprüfung nicht. Wenn Sie die Route 53-Konsole verwenden, geben Sie die Zeichenfolge in das Feld Search String (Suchzeichenfolge) ein. Wenn Sie die Route 53-API verwenden, geben Sie die Zeichenfolge beim Erstellen der Zustandsprüfung in das Element `SearchString` ein.

Wenn bei Integritätsprüfungen, die einen Endpunkt überwachen (mit Ausnahme von TCP-Integritätsprüfungen), die Antwort des Endpunkts Header enthält, müssen die Header das Format haben, das in RFC723 0, Hypertext Transfer Protocol (HTTP/1.1): Nachrichtensyntax und Routing, Abschnitt 3.2, „Header-Felder“, definiert ist.

Route 53 betrachtet eine neue Zustandsprüfung als fehlerfrei, bis genügend Daten zur Ermittlung des tatsächlichen Status (fehlerfrei oder fehlerhaft) vorliegen. Wenn Sie die Option zur Umkehrung des Zustandsprüfungsstatus wählen, wird eine neue Zustandsprüfung von Route 53 als fehlerhaft betrachtet, bis genügend Daten vorliegen.

So ermittelt Route 53 den Status von Zustandsprüfungen zur Überwachung anderer Zustandsprüfungen

Eine Zustandsprüfung kann den Status anderer Zustandsprüfungen überwachen. Diese Art der Zustandsprüfung wird als berechnete Zustandsprüfung bezeichnet. Die Zustandsprüfung, die die Überwachung ausführt, ist die übergeordnete Zustandsprüfung, und die Zustandsprüfungen, die überwacht werden, sind untergeordnete Zustandsprüfungen. Eine übergeordnete Zustandsprüfung kann den Zustand von bis zu 255 untergeordneten Zustandsprüfungen überwachen. So funktioniert die Überwachung:

- Route 53 addiert die Anzahl der untergeordneten Zustandsprüfungen, die als fehlerfrei gelten.
- Route 53 vergleicht diese Anzahl mit der Anzahl der untergeordneten Zustandsprüfungen, die fehlerfrei sein müssen, damit die übergeordnete Zustandsprüfung als fehlerfrei bewertet wird.

Weitere Informationen finden Sie unter Überwachung anderer Zustandsprüfungen (Berechnete Zustandsprüfungen) in Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.

Route 53 betrachtet eine neue Zustandsprüfung als fehlerfrei, bis genügend Daten zur Ermittlung des tatsächlichen Status (fehlerfrei oder fehlerhaft) vorliegen. Wenn Sie die Option zur Umkehrung des Zustandsprüfungsstatus wählen, wird eine neue Zustandsprüfung von Route 53 als fehlerhaft betrachtet, bis genügend Daten vorliegen.

Wie Route 53 den Status von Integritätsprüfungen bestimmt, die Alarme überwachen CloudWatch

Wenn Sie eine Zustandsprüfung erstellen, die auf einem CloudWatch Alarm basiert, überwacht Route 53 den Datenstrom für den entsprechenden Alarm, anstatt den Alarmstatus zu überwachen.

Wenn der Datenstrom anzeigt, dass der Alarmzustand OK ist, wird die Zustandsprüfung als stabil betrachtet. Wenn der Datenstrom anzeigt, dass der Zustand Alarm ist, wird die Zustandsprüfung als instabil betrachtet. Wenn der Datenstrom nicht genügend Informationen liefert, um den Status des Alarms zu ermitteln, hängt der Status der Statusprüfung von der Einstellung für Health check status ab: stabil, instabil oder zuletzt bekannter Status. (In der Route 53-API ist diese Einstellung `InsufficientDataHealthStatus`.)

Route 53 unterstützt keine kontenübergreifenden CloudWatch Alarme.

> **Note**
>
> Da Route 53-Zustandsprüfungen CloudWatch Datenströme und nicht den Status von CloudWatch Alarmen überwachen, können Sie mithilfe des CloudWatch SetAlarmStateAPI-Vorgangs nicht erzwingen, dass sich der Status einer Integritätsprüfung ändert.

Route 53 betrachtet eine neue Zustandsprüfung als fehlerfrei, bis genügend Daten zur Ermittlung des tatsächlichen Status (fehlerfrei oder fehlerhaft) vorliegen. Wenn Sie die Option zur Umkehrung des Zustandsprüfungsstatus wählen, wird eine neue Zustandsprüfung von Route 53 als fehlerhaft betrachtet, bis genügend Daten vorliegen.

Erstellen, Aktualisieren und Löschen von Zustandsprüfungen

> **Important**
>
> Wenn Sie Zustandsprüfungen aktualisieren oder löschen, die im Zusammenhang mit Datensätzen stehen, überprüfen Sie die Aufgaben in Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover, bevor Sie fortfahren.

In diesem Abschnitt werden die folgenden Themen im Zusammenhang mit der Verwaltung von Route 53-Zustandsprüfungen behandelt:

1. Integritätsprüfungen erstellen und aktualisieren:
   - Erfahren Sie, wie Sie mithilfe der Route 53-Konsole Integritätsprüfungen erstellen und aktualisieren.

- Machen Sie sich mit den Werten vertraut, die Sie bei der Erstellung oder Aktualisierung von Integritätsprüfungen angeben müssen, z. B. Endpunktüberwachung, Protokoll, IP-Adresse, Domänenname und erweiterte Konfigurationsoptionen.

2. Werte, die bei der Erstellung einer Integritätsprüfung angezeigt werden:
   - Entdecken Sie die Werte, die die Route 53-Konsole auf der Grundlage Ihrer Eingaben bei der Erstellung einer Integritätsprüfung anzeigt, z. B. die vollständige URL oder IP-Adresse und den Port.
3. Aktualisierung der Zustandsprüfungen für CloudWatch Alarmanpassungen:
   - Erfahren Sie, wie Sie einen Gesundheitscheck aktualisieren können, wenn Sie die Einstellungen des zugehörigen CloudWatch Alarms ändern.
4. Gesundheitschecks löschen:
   - Folgen Sie dem Verfahren zum Löschen von Integritätsprüfungen mithilfe der Route 53-Konsole.
5. Aktualisieren oder Löschen von Integritätsprüfungen, wenn DNS-Failover konfiguriert ist:
   - Machen Sie sich mit den empfohlenen Aufgaben vertraut, die Sie beim Aktualisieren oder Löschen von Integritätsprüfungen im Zusammenhang mit DNS-Einträgen ausführen sollten, um eine korrekte Routing- und Failover-Konfiguration sicherzustellen.
6. Konfiguration von Router- und Firewallregeln:
   - Erfahren Sie, wie Sie Ihre Router- und Firewallregeln so konfigurieren, dass eingehender Datenverkehr von Route 53-Zustandsprüfern zugelassen wird, sodass erfolgreiche Integritätsprüfungen gewährleistet sind.

Wenn Sie die Informationen in diesem Abschnitt befolgen, können Sie Route 53-Zustandsprüfungen effektiv erstellen, aktualisieren und löschen, deren Konfiguration verwalten und die ordnungsgemäße Integration mit DNS-Failover- und Routing-Richtlinien sicherstellen.

Themen

- Löschen von Zustandsprüfungen
- Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover
- Konfigurieren von Router- und Firewall-Regeln für Amazon Route 53-Zustandsprüfungen

Erstellen und Aktualisieren von Zustandsprüfungen

Das folgende Verfahren erläutert, wie Sie Zustandsprüfungen mit der Route 53-Konsole erstellen und aktualisieren.

> **Note**
>
> Wir aktualisieren die Konsole für Integritätsprüfungen für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Um einen Integritätscheck zu erstellen oder zu aktualisieren

1. Wenn Sie Zustandsprüfungen aktualisieren, die im Zusammenhang mit Datensätzen stehen, führen Sie die empfohlenen Aufgaben in Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover aus.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Wählen Sie im Navigationsbereich Health Checks aus.
4. Wenn Sie eine bestehende Zustandsprüfung aktualisieren möchten, wählen Sie die verknüpfte ID der Zustandsprüfung und dann Bearbeiten aus.

   Wenn Sie einen Gesundheitscheck erstellen möchten, wählen Sie Gesundheitscheck erstellen.

5. Geben Sie die entsprechenden Werte ein. Beachten Sie, dass einige Werte nicht mehr geändert werden können, nachdem Sie eine Zustandsprüfung erstellt haben. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.
6. Wählen Sie Zustandsprüfung erstellen aus.

> **Note**
>
> Route 53 betrachtet eine neue Zustandsprüfung als fehlerfrei, bis genügend Daten zur Ermittlung des tatsächlichen Status (fehlerfrei oder fehlerhaft) vorliegen.

7. Verknüpfen Sie die Zustandsprüfung mit mindestens einem Route 53-Datensatz. Informationen zur Erstellung und Aktualisierung von Datensätzen finden Sie unter Arbeiten mit Datensätzen.

Old console

Um einen Gesundheitscheck zu erstellen oder zu aktualisieren

1. Wenn Sie Zustandsprüfungen aktualisieren, die im Zusammenhang mit Datensätzen stehen, führen Sie die empfohlenen Aufgaben in Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover aus.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Wählen Sie im Navigationsbereich Health Checks aus.
4. Wenn Sie eine vorhandene Zustandsprüfung aktualisieren möchten, wählen Sie die Zustandsprüfung aus, und klicken Sie anschließend auf Edit Health Check.

   Wenn Sie eine Zustandsprüfung erstellen möchten, wählen Sie Create Health Check. Weitere Informationen über Einstellungen erhalten Sie in Quickinfos, wenn Sie den Mauszeiger über die jeweilige Beschriftung bewegen.
5. Geben Sie die entsprechenden Werte ein. Beachten Sie, dass einige Werte nicht mehr geändert werden können, nachdem Sie eine Zustandsprüfung erstellt haben. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.
6. Wählen Sie Create Health Check.

> **Note**
>
> Route 53 betrachtet eine neue Zustandsprüfung als fehlerfrei, bis genügend Daten zur Ermittlung des tatsächlichen Status (fehlerfrei oder fehlerhaft) vorliegen. Wenn Sie die Option zur Umkehrung des Zustandsprüfungsstatus wählen, wird eine neue Zustandsprüfung von Route 53 als fehlerhaft betrachtet, bis genügend Daten vorliegen.

7. Verknüpfen Sie die Zustandsprüfung mit mindestens einem Route 53-Datensatz. Informationen zur Erstellung und Aktualisierung von Datensätzen finden Sie unter Arbeiten mit Datensätzen.

Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen

Wenn Sie Zustandsprüfungen erstellen oder aktualisieren, legen Sie die entsprechenden Werte fest. Beachten Sie, dass einige Werte nicht mehr geändert werden können, nachdem Sie eine Zustandsprüfung erstellt haben.

Themen

- Überwachung eines Endpunkts
- Überwachung anderer Zustandsprüfungen (Berechnete Zustandsprüfungen)
- Überwachung von CloudWatch-Alarmen
- Erweiterte Konfiguration (nur "Monitor an endpoint")
- Eine Benachrichtigung erhalten, wenn eine Zustandsprüfung fehlschlägt

Name

Optional, aber empfohlen: Der Name, den Sie der Zustandsprüfung geben wollen. Wenn Sie einen Wert für Name festlegen, versieht Route 53 die Zustandsprüfung mit einem Tag, weist dem Tag-Schlüssel den Wert Name zu und weist den Wert, den Sie festlegen, dem Tagwert zu. Der Wert des Tags Name erscheint in der Liste der Zustandsprüfungen in der Route 53-Konsole, mit der Sie Zustandsprüfungen auf einfache Weise unterscheiden können.

Weitere Informationen zu Markieren und Zustandsprüfungen finden Sie unter Benennen und Verwenden von Tags für Zustandsprüfungen.

Was Sie überwachen sollten

Ganz gleich, ob Sie möchten, dass diese Zustandsprüfung einen Endpunkt oder den Status anderer Zustandsprüfungen überwacht:

- Endpoint - Route 53 überwacht den Zustand eines Endpunktes, den Sie angeben. Sie können den Endpunkt angeben, indem Sie entweder einen Domänennamen oder eine IP-Adresse und einen Port bereitstellen.

  > **Note**
  >
  > Wenn Sie einen AWS Nicht-Endpunkt angeben, fällt eine zusätzliche Gebühr an. Weitere Informationen, darunter eine Definition von AWS -Endpunkten, finden Sie im Bereich "Zustandsprüfungen" auf der Seite Route 53 – Preise.

- Status anderer Zustandsprüfungen (berechnete Zustandsprüfung) - Route 53 bestimmt anhand des Status anderer von Ihnen festgelegten Zustandsprüfungen, ob diese Zustandsprüfung fehlerfrei ist. Sie können auch angeben, wie viele Zustandsprüfungen fehlerfrei sein müssen, damit diese Zustandsprüfung als fehlerfrei angesehen wird.
- Status des CloudWatch Alarm-Datenstroms — Route 53 bestimmt, ob diese Zustandsprüfung fehlerfrei ist, indem sie den Datenstrom auf einen CloudWatch Alarm überwacht.

Überwachung eines Endpunkts

> **Note**
>
> Wir aktualisieren die Konsole für die Zustandsprüfungen für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Wenn Sie möchten, dass diese Zustandsprüfung einen Endpunkt überwacht, geben Sie die folgenden Werte an:

- Geben Sie Endpunkte an nach
- IP-Adresse
- Domain-Name

Legen Sie den Endpunkt wie folgt fest

Ob Sie den Endpunkt mit einer IP-Adresse oder einem Domänennamen festlegen möchten.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Specify endpoint by nicht mehr ändern.

IP-Adresse (nur "Specify endpoint by IP address")

Wählen Sie das Protokoll in der Dropdownliste aus und geben Sie die IP-Adresse, den Port und den Pfad in das Textfeld ein.

- Das Protokoll kann eines der folgenden sein:

  HTTP: Route 53 versucht, eine TCP-Verbindung herzustellen. Bei einem erfolgreichen Verbindungsversuch sendet Route 53 eine HTTP-Anforderung und wartet auf einen HTTP-Statuscode von 2xx oder 3xx.

- HTTPS: Route 53 versucht, eine TCP-Verbindung herzustellen. Bei einem erfolgreichen Verbindungsversuch sendet Route 53 eine HTTPS-Anforderung und wartet auf einen HTTP-Statuscode von 2xx oder 3xx.

  > **Important**
  >
  > Wenn Sie HTTPS wählen, muss der Endpunkt TLS v1.0, v1.1 oder v1.2 unterstützen.

  Wenn Sie HTTPS für den Wert von Protokoll auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

- TCP - Route 53 versucht, eine TCP-Verbindung herzustellen.

Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Protocol nicht mehr ändern.

Als IP-Adresse können Sie eine IPv4 IPv6 Oder-Adresse des Endpunkts eingeben, auf dem Route 53 Integritätsprüfungen durchführen soll, wenn Sie Endpunkt nach IP-Adresse angeben ausgewählt haben.

Route 53 kann den Zustand von Endpunkten, für die die IP-Adresse im lokalen, privaten, nicht-routingfähigen oder Multicast-Bereich liegt, nicht überprüfen. Weitere Informationen über IP-Adressen, für die Sie keine Zustandsprüfungen erstellen können, finden Sie in den folgenden Dokumenten:

- RFC 5735, Adressen für besondere Verwendungszwecke IPv4
- RFC 6598, IPv4 IANA-reserviertes Präfix für gemeinsam genutzten Adressraum.
- RFC 5156, Adressen für besondere Zwecke IPv6

Wenn der Endpunkt eine EC2 Amazon-Instance ist, empfehlen wir Ihnen, eine Elastic IP-Adresse zu erstellen, sie Ihrer EC2 Instance zuzuordnen und die Elastic IP-Adresse anzugeben. Auf diese Weise wird sichergestellt, dass sich die IP-Adresse Ihrer Instance nicht mehr ändert. Weitere Informationen finden Sie unter Elastic IP Addresses (EIP) im EC2 Amazon-Benutzerhandbuch.

Wenn Sie die EC2 Amazon-Instance löschen, stellen Sie sicher, dass Sie auch die mit der EIP verknüpfte Zustandsprüfung löschen. Weitere Informationen finden Sie unter Bewährte Methoden für Amazon Route 53 Zustandsprüfungen.

> **Note**
>
> Wenn Sie einen AWS Nicht-Endpunkt angeben, fällt eine zusätzliche Gebühr an. Weitere Informationen, darunter eine Definition von AWS -Endpunkten, finden Sie im Bereich "Zustandsprüfungen" auf der Seite Route 53 – Preise.

Für den Port geben Sie den Port auf dem Endpunkt ein, auf dem Route 53 Integritätsprüfungen durchführen soll.

Für den Pfad (nur HTTP- und HTTPS-Protokolle) geben Sie den Pfad ein, den Route 53 bei der Durchführung von Integritätsprüfungen anfordern soll. Der Pfad kann ein beliebiger Wert sein, für den Ihr Endpunkt den H-TTP-Statuscode 2xx oder 3xx zurückgibt, wenn der Endpunkt fehlerfrei ist, z. B. die Datei/.html? docs/route53-health-check.html. You can also include query string parameters, for example, /welcome language=jp&login=y. Wenn Sie keinen führenden Schrägstrich (/) angeben, fügt Route 53 automatisch einen hinzu.

Domänenname (Nur "Specify endpoint by domain name", Alle Protokolle)

Der Domänenname (example.com) oder Unterdomänenname (backend.example.com) des Endpunkts, für den Route 53 Zustandsprüfungen durchführen soll, wenn Sie Specify endpoint by domain name auswählen.

Wenn Sie den Endpunkt nach dem Domänennamen angeben, sendet Route 53 eine DNS-Abfrage zur Auflösung des Domänenamens, den Sie in Domain name festlegen, in dem von Ihnen unter Request interval angegebenen Intervall. Unter Verwendung einer IPv4-Adresse, die DNS zurücksendet, überprüft Route 53 anschließend den Zustand des Endpunkts.

> **Note**
>
> Wenn Sie den Endpunkt anhand des Domänennamens angeben, verwendet Route 53 nur, IPv4 um Integritätsprüfungen an den Endpunkt zu senden. Wenn es keinen Datensatz mit Typ A für den Namen gibt, den Sie für Domain name angeben, schlägt die Zustandsprüfung mit dem Fehler „DNS resolution failed“ fehl.

Wenn Sie den Status von Failover-, Geolocation-, Geoproximity-, Latenz-, mehrwertigen oder gewichteten Datensätzen prüfen und den Endpunkt über den Domänennamen festlegen möchten, empfehlen wir die Erstellung einer eigenen Statusprüfung für jeden Endpunkt. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Geben Sie als Wert von Domain name den Domänennamen des Servers an (z. B. us-east-2-www.example.com), nicht den Namen des Datensatzes (www.example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend

die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Wenn darüber hinaus der Wert für Protocol HTTP oder HTTPS ist, gibt Route 53 den Wert für Domain name in der `Host` Kopfzeile an. Einzelheiten dazu finden Sie unter Host name weiter oben in dieser Liste. Wenn der Wert von Protocol TCP ist, übergibt Route 53 keine `Host`-Kopfzeile.

> **Note**
>
> Wenn Sie einen AWS Nicht-Endpunkt angeben, fällt eine zusätzliche Gebühr an. Weitere Informationen, darunter eine Definition von AWS -Endpunkten, finden Sie im Bereich "Zustandsprüfungen" auf der Seite Route 53 – Preise.

Old console

Wenn Sie möchten, dass diese Zustandsprüfung einen Endpunkt überwacht, geben Sie die folgenden Werte an:

- Legen Sie den Endpunkt wie folgt fest
- Protokoll
- IP-Adresse
- Host name
- Port
- Domain-Name
- Pfad

Legen Sie den Endpunkt wie folgt fest

Ob Sie den Endpunkt mit einer IP-Adresse oder einem Domänennamen festlegen möchten.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Specify endpoint by nicht mehr ändern.

Protokoll

Die Methode, die Route 53 nutzen soll, um den Zustand Ihres Endpunktes zu überwachen:

- HTTP: Route 53 versucht, eine TCP-Verbindung herzustellen. Bei einem erfolgreichen Verbindungsversuch sendet Route 53 eine HTTP-Anforderung und wartet auf einen HTTP-Statuscode von 2xx oder 3xx.
- HTTPS: Route 53 versucht, eine TCP-Verbindung herzustellen. Bei einem erfolgreichen Verbindungsversuch sendet Route 53 eine HTTPS-Anforderung und wartet auf einen HTTP-Statuscode von 2xx oder 3xx.

> **Important**
>
> Wenn Sie HTTPS wählen, muss der Endpunkt TLS v1.0, v1.1 oder v1.2 unterstützen.

Wenn Sie HTTPS für den Wert von Protokoll auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

- TCP - Route 53 versucht, eine TCP-Verbindung herzustellen.

Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Protocol nicht mehr ändern.

IP-Adresse (nur "Specify endpoint by IP address")

Die IPv4 oder IPv6 Adresse des Endpunkts, auf dem Route 53 Integritätsprüfungen durchführen soll, wenn Sie Endpunkt nach IP-Adresse angeben ausgewählt haben.

Route 53 kann den Zustand von Endpunkten, für die die IP-Adresse im lokalen, privaten, nicht-routingfähigen oder Multicast-Bereich liegt, nicht überprüfen. Weitere Informationen über IP-Adressen, für die Sie keine Zustandsprüfungen erstellen können, finden Sie in den folgenden Dokumenten:

- RFC 5735, Adressen für besondere Zwecke IPv4
- RFC 6598, IPv4 IANA-reserviertes Präfix für gemeinsam genutzten Adressraum.
- RFC 5156, Adressen für besondere Zwecke IPv6

Wenn der Endpunkt eine EC2 Amazon-Instance ist, empfehlen wir Ihnen, eine Elastic IP-Adresse zu erstellen, sie Ihrer EC2 Instance zuzuordnen und die Elastic IP-Adresse anzugeben. Auf diese Weise wird sichergestellt, dass sich die IP-Adresse Ihrer Instance nicht mehr ändert. Weitere Informationen finden Sie unter Elastic IP Addresses (EIP) im EC2 Amazon-Benutzerhandbuch.

Wenn Sie die EC2 Amazon-Instance löschen, stellen Sie sicher, dass Sie auch die mit der EIP verknüpfte Zustandsprüfung löschen. Weitere Informationen finden Sie unter Bewährte Methoden für Amazon Route 53 Zustandsprüfungen.

> **Note**
>
> Wenn Sie einen AWS Nicht-Endpunkt angeben, fällt eine zusätzliche Gebühr an. Weitere Informationen, darunter eine Definition von AWS -Endpunkten, finden Sie im Bereich "Zustandsprüfungen" auf der Seite Route 53 – Preise.

Host-Name (nur "Specify endpoint by IP address", nur HTTP- und HTTPS-Protokolle)

Der Wert, den Route 53 in der `Host`-Kopfzeile in HTTP- und HTTPS-Zustandsprüfungen angeben soll. Dies ist in der Regel der vollqualifizierte DNS-Name der Website, auf der Route 53 Zustandsprüfungen durchführen soll. Wenn Route 53 den Zustand eines Endpunkts überprüft, erstellt es den `Host`-Header folgendermaßen:

- Wenn Sie einen Wert von **`80`** für Port und von HTTP für Protocol festlegen, übergibt Route 53 an den Endpunkt eine `Host`-Kopfzeile, die den Wert Host name enthält.
- Wenn Sie einen Wert von **`443`** für Port und von HTTPS für Protocol festlegen, übergibt Route 53 an den Endpunkt eine `Host`-Kopfzeile, die den Wert Host name enthält.
- Wenn Sie einen anderen Wert für Port und entweder HTTP oder HTTPS für Protokoll angeben, leitet Route 53 einen `Host` Header an den Endpunkt weiter, der den Wert enthält *`Host name`*:*`Port`*.

Wenn Sie sich dafür entscheiden, den Endpunkt durch die IP-Adresse anzugeben, und Sie keinen Wert für Host name festlegen, ersetzt Route 53 IP address in der -`Host`Kopfzeile in allen vorangegangenen Fällen.

Port

Der Port am Endpunkt, für den Amazon Route 53 Zustandsprüfungen durchführen soll.

Domänenname (Nur "Specify endpoint by domain name", Alle Protokolle)

Der Domänenname (example.com) oder Unterdomänenname (backend.example.com) des Endpunkts, für den Route 53 Zustandsprüfungen durchführen soll, wenn Sie Specify endpoint by domain name auswählen.

Wenn Sie den Endpunkt nach dem Domänennamen angeben, sendet Route 53 eine DNS-Abfrage zur Auflösung des Domänenamens, den Sie in Domain name festlegen, in dem von Ihnen unter Request interval angegebenen Intervall. Unter Verwendung einer IPv4-Adresse, die DNS zurücksendet, überprüft Route 53 anschließend den Zustand des Endpunkts.

> **Note**
>
> Wenn Sie den Endpunkt anhand des Domänennamens angeben, verwendet Route 53 nur, IPv4 um Integritätsprüfungen an den Endpunkt zu senden. Wenn es keinen Datensatz mit Typ A für den Namen gibt, den Sie für Domain name angeben, schlägt die Zustandsprüfung mit dem Fehler „DNS resolution failed“ fehl.

Wenn Sie den Status von Failover-, Geolocation-, Geoproximity-, Latenz-, mehrwertigen oder gewichteten Datensätzen prüfen und den Endpunkt über den Domänennamen festlegen möchten, empfehlen wir die Erstellung einer eigenen Statusprüfung für jeden Endpunkt. Sie sollten beispielsweise eine Zustandsprüfung für jeden HTTP-Server erstellen, der Inhalte für www.example.com bereitstellt. Geben Sie als Wert von Domain name den Domänennamen des Servers an (z. B. us-east-2-www.example.com), nicht den Namen des Datensatzes (www.example.com).

> **Important**
>
> Wenn Sie in dieser Konfiguration eine Zustandsprüfung erstellen, für die der Wert von Domain name dem Namen des Datensatzes entspricht, und anschließend die Zustandsprüfung mit diesen Datensätzen verknüpfen, sind die Ergebnisse der Zustandsprüfung unvorhersehbar.

Wenn darüber hinaus der Wert für Protocol HTTP oder HTTPS ist, gibt Route 53 den Wert für Domain name in der `Host` Kopfzeile an. Einzelheiten dazu finden Sie unter Host name weiter oben in dieser Liste. Wenn der Wert von Protocol TCP ist, übergibt Route 53 keine `Host`-Kopfzeile.

> **Note**
>
> Wenn Sie einen AWS Nicht-Endpunkt angeben, fällt eine zusätzliche Gebühr an. Weitere Informationen, darunter eine Definition von AWS -Endpunkten, finden Sie im Bereich "Zustandsprüfungen" auf der Seite Route 53 – Preise.

Pfad (nur HTTP- und HTTPS-Protokolle)

Der Pfad, den Route 53 bei der Ausführung von Integritätsprüfungen anfordern soll. Der Pfad kann ein beliebiger Wert sein, für den der Endpunkt einen HTTP-Statuscode `2xx` oder `3xx` herausgibt, wenn der Endpunkt fehlerfrei ist, z. B. die Datei `/docs/route53-health-check.html`. Sie können auch Abfragezeichenfolgenparameter einschließen, z. B. `/welcome.html?language=jp&login=y`. Wenn Sie keinen führenden Schrägstrich (`/`) angeben, fügt Route 53 automatisch einen ein.

Überwachung anderer Zustandsprüfungen (Berechnete Zustandsprüfungen)

> **Note**
>
> Wir aktualisieren die Health Checks Console für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Wenn Sie möchten, dass diese Zustandsprüfung den Status anderer Zustandsprüfungen überwacht, legen Sie die folgenden Werte fest:

- Zu überwachende Zustandsprüfungen
- Bericht fehlerfrei, wenn

Zu überwachende Zustandsprüfungen

Die Zustandsprüfungen, die Route 53 überwachen soll, um den Zustand dieser Zustandsprüfung zu bestimmen.

Sie können bis zu 256 Zustandsprüfungen zur Kategorie Health checks to monitor hinzufügen. Um eine Zustandsprüfung aus der Liste zu entfernen, wählen Sie das x am rechten Ende der Markierung für diese Zustandsprüfung aus.

> **Note**
>
> Sie können eine berechnete Zustandsprüfung nicht so konfigurieren, dass sie den Zustand anderer berechneter Zustandsprüfungen überwacht.

Wenn Sie eine Zustandsprüfung deaktivieren, mit der eine berechnete Zustandsprüfung überwacht wird, stuft Route 53 die deaktivierte Zustandsprüfung als fehlerfrei ein, wenn berechnet wird, ob die berechnete Zustandsprüfung fehlerfrei ist. Wenn Sie möchten, dass die deaktivierte Zustandsprüfung als fehlerhaft eingestuft wird, aktivieren Sie das Kontrollkästchen Invert health check status (Status der Zustandsprüfung umkehren).

Bericht fehlerfrei, wenn

Die Berechnung, die Route 53 ausführen soll, um festzustellen, ob diese Zustandsprüfung fehlerfrei ist:

- Report healthy when at least x of y selected health checks are healthy - Route 53 betrachtet diese Zustandsprüfung als fehlerfrei, wenn die angegebene Anzahl von Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei ist. Beachten Sie Folgendes:
  - Wenn Sie eine Zahl festlegen, die größer als die Anzahl der Zustandsprüfungen in der Kategorie Health checks to monitor ist, sieht Route 53 diese Zustandsprüfung immer als fehlerhaft an.
  - Wenn Sie 0 angeben, betrachtet Route 53 diese Zustandsprüfung immer als fehlerfrei.
- Report healthy when all health checks are healthy (AND) - Route 53 betrachtet diese Zustandsprüfung nur dann als fehlerfrei, wenn alle Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei sind.

- Report healthy when one or more health checks are healthy (OR) - Route 53 betrachtet diese Zustandsprüfung als fehlerfrei, wenn mindestens eine der Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei ist.

Old console

Wenn Sie möchten, dass diese Zustandsprüfung den Status anderer Zustandsprüfungen überwacht, legen Sie die folgenden Werte fest:

- Zu überwachende Zustandsprüfungen
- Bericht fehlerfrei, wenn
- Status der Zustandsprüfung umkehren
- Disabled

Zu überwachende Zustandsprüfungen

Die Zustandsprüfungen, die Route 53 überwachen soll, um den Zustand dieser Zustandsprüfung zu bestimmen.

Sie können bis zu 256 Zustandsprüfungen zur Kategorie Health checks to monitor hinzufügen. Um eine Zustandsprüfung aus der Liste zu entfernen, wählen Sie das x am rechten Ende der Markierung für diese Zustandsprüfung aus.

> **Note**
>
> Sie können eine berechnete Zustandsprüfung nicht so konfigurieren, dass sie den Zustand anderer berechneter Zustandsprüfungen überwacht.

Wenn Sie eine Zustandsprüfung deaktivieren, mit der eine berechnete Zustandsprüfung überwacht wird, stuft Route 53 die deaktivierte Zustandsprüfung als fehlerfrei ein, wenn berechnet wird, ob die berechnete Zustandsprüfung fehlerfrei ist. Wenn Sie möchten, dass die deaktivierte Zustandsprüfung als fehlerhaft eingestuft wird, aktivieren Sie das Kontrollkästchen Invert health check status (Status der Zustandsprüfung umkehren).

Bericht fehlerfrei, wenn

Die Berechnung, die Route 53 ausführen soll, um festzustellen, ob diese Zustandsprüfung fehlerfrei ist:

- Report healthy when at least x of y selected health checks are healthy - Route 53 betrachtet diese Zustandsprüfung als fehlerfrei, wenn die angegebene Anzahl von Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei ist. Beachten Sie Folgendes:
  - Wenn Sie eine Zahl festlegen, die größer als die Anzahl der Zustandsprüfungen in der Kategorie Health checks to monitor ist, sieht Route 53 diese Zustandsprüfung immer als fehlerhaft an.
  - Wenn Sie 0 angeben, betrachtet Route 53 diese Zustandsprüfung immer als fehlerfrei.
- Report healthy when all health checks are healthy (AND) - Route 53 betrachtet diese Zustandsprüfung nur dann als fehlerfrei, wenn alle Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei sind.
- Report healthy when one or more health checks are healthy (OR) - Route 53 betrachtet diese Zustandsprüfung als fehlerfrei, wenn mindestens eine der Zustandsprüfungen, die Sie zur Kategorie Health checks to monitor hinzugefügt haben, fehlerfrei ist.

Den Status der Integritätsprüfung umkehren (nur alte Konsole)

Informationen zum Umkehren einer Systemdiagnose auf der neuen Konsole finden Sie unter. Integritätsprüfungen rückgängig machen

Wählen Sie, ob Sie möchten, dass Route 53 den Status einer Zustandsprüfung umkehrt. Wenn Sie diese Option auswählen, betrachtet Route 53 Zustandsprüfungen als fehlerhaft, wenn sie den Status "fehlerfrei" aufweisen, und umgekehrt.

Deaktiviert (nur alte Konsole)

Informationen zum Deaktivieren einer Systemdiagnose auf der neuen Konsole finden Sie unterGesundheitschecks deaktivieren oder aktivieren.

Stoppt die Ausführung von Zustandsprüfungen durch Route 53. Wenn Sie eine Zustandsprüfung deaktivieren, wird die Aggregation des Status der referenzierten Zustandsprüfungen durch Route 53 gestoppt.

Nachdem eine Zustandsprüfung deaktiviert wurde, stuft Route 53 den Status der Zustandsprüfung immer als fehlerfrei ein. Wenn Sie ein DNS Failover konfiguriert haben, leitet Route 53 weiterhin Datenverkehr an die entsprechenden Ressourcen weiter. Wenn Sie die Weiterleitung von Datenverkehr zu einer Ressource beenden möchten, kehren Sie die Zustandsprüfung um.

> **Note**
>
> Gebühren für eine Zustandsprüfung gelten weiterhin, auch wenn die Zustandsprüfung deaktiviert ist.

Überwachung von CloudWatch-Alarmen

> **Note**
>
> Wir aktualisieren die Health Checks-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Wenn mit dieser Integritätsprüfung der Alarmstatus eines CloudWatch Alarms überwacht werden soll, geben Sie die folgenden Werte an:

- CloudWatch Alarm
- Status der Zustandsprüfung

CloudWatch Alarm

Wählen Sie den CloudWatch Alarm aus, den Route 53 verwenden soll, um festzustellen, ob diese Zustandsprüfung fehlerfrei ist. Der CloudWatch Alarm muss mit dem Gesundheitscheck AWS-Konto identisch sein.

> **Note**
>
> Route 53 unterstützt CloudWatch Alarme mit den folgenden Funktionen:

- Metriken mit Standardauflösung. Metriken mit hoher Auflösung werden nicht unterstützt. Weitere Informationen finden Sie unter Metriken mit hoher Auflösung im CloudWatch Amazon-Benutzerhandbuch.
- Statistik: `Average`, `Minimum`, `Maximum`, `Sum` und `SampleCount`. Erweiterte Statistiken werden nicht unterstützt.
- „M von N“ -Alarme werden von Route 53 nicht unterstützt. Weitere Informationen finden Sie im CloudWatch Amazon-Leitfaden unter Einen Alarm auswerten.

Route 53 unterstützt keine Alarme, die metrische Mathematik verwenden, um mehrere CloudWatch Metriken abzufragen.

Führen Sie zum Erstellen eines Alarms folgende Schritte aus:

1. Wählen Sie „Erstellen“. Die CloudWatch Konsole wird in einem neuen Browser-Tab angezeigt.
2. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Einen CloudWatch Alarm erstellen oder bearbeiten im CloudWatch Amazon-Benutzerhandbuch.
3. Kehren Sie zur Browser-Registerkarte zurück, auf der die Route 53-Konsole angezeigt wird.
4. Wählen Sie die Schaltfläche „Aktualisieren“ neben der CloudWatchAlarmliste.
5. Wählen Sie den neuen Alarm aus der Liste aus.

Important

Wenn Sie die Einstellungen für den CloudWatch Alarm ändern, nachdem Sie eine Zustandsprüfung erstellt haben, müssen Sie die Zustandsprüfung aktualisieren. Weitere Informationen finden Sie unter Aktualisierung der Gesundheitschecks, wenn Sie die CloudWatch Alarmeinstellungen ändern (Zustandsprüfungen, die nur einen CloudWatch Alarm überwachen).

Status der Zustandsprüfung

Wählen Sie den Status der Zustandsprüfung (gesund, fehlerhaft oder letzter bekannter Status), wenn CloudWatch nicht genügend Daten vorliegen, um den Status des Alarms zu bestimmen, den Sie für den CloudWatchAlarm ausgewählt haben. Wenn Sie sich dafür entscheiden, den

letzten bekannten Status zu verwenden, verwendet Route 53 den Status der Zustandsprüfung von dem Zeitpunkt, zu dem das letzte Mal genügend Daten zur Verfügung CloudWatch standen, um den Alarmstatus zu bestimmen. Bei neuen Zustandsprüfungen, die keinen letzten bekannten Status haben, ist der Standardstatus für die Zustandsprüfung „fehlerfrei“.

Der Wert Health Check Status bietet einen temporären Status, wenn der Datenstream für eine CloudWatch Metrik kurzzeitig nicht verfügbar ist. (Route 53 überwacht Datenströme auf CloudWatch Messwerte, nicht auf den Status des entsprechenden Alarms.) Wenn die Metrik häufig oder für lange Zeit (länger als ein paar Stunden) nicht verfügbar ist, empfehlen wir Ihnen, den letzten bekannten Status nicht zu verwenden.

Old console

Wenn mit dieser Integritätsprüfung der Alarmstatus eines CloudWatch Alarms überwacht werden soll, geben Sie die folgenden Werte an:

- CloudWatch Alarm
- Status der Zustandsprüfung
- Status der Zustandsprüfung umkehren
- Disabled

CloudWatch Alarm

Wählen Sie den CloudWatch Alarm aus, den Route 53 verwenden soll, um festzustellen, ob diese Zustandsprüfung fehlerfrei ist. Der CloudWatch Alarm muss mit dem Gesundheitscheck AWS-Konto identisch sein.

> **Note**
>
> Route 53 unterstützt CloudWatch Alarme mit den folgenden Funktionen:
>
> - Metriken mit Standardauflösung. Metriken mit hoher Auflösung werden nicht unterstützt. Weitere Informationen finden Sie unter Metriken mit hoher Auflösung im CloudWatch Amazon-Benutzerhandbuch.
> - Statistik: `Average`, `Minimum`, `Maximum`, `Sum` und `SampleCount`. Erweiterte Statistiken werden nicht unterstützt.
> - „M von N“ -Alarme werden von Route 53 nicht unterstützt. Weitere Informationen finden Sie im CloudWatch Amazon-Leitfaden unter Einen Alarm auswerten.

Route 53 unterstützt keine Alarme, die metrische Mathematik verwenden, um mehrere CloudWatch Metriken abzufragen.

Führen Sie zum Erstellen eines Alarms folgende Schritte aus:

1. Wählen Sie „Erstellen“. Die CloudWatch Konsole wird in einem neuen Browser-Tab angezeigt.
2. Geben Sie die entsprechenden Werte ein. Weitere Informationen finden Sie unter Einen CloudWatch Alarm erstellen oder bearbeiten im CloudWatch Amazon-Benutzerhandbuch.
3. Kehren Sie zur Browser-Registerkarte zurück, auf der die Route 53-Konsole angezeigt wird.
4. Wählen Sie die Schaltfläche „Aktualisieren“ neben der CloudWatchAlarmliste.
5. Wählen Sie den neuen Alarm aus der Liste aus.

Important

Wenn Sie die Einstellungen für den CloudWatch Alarm ändern, nachdem Sie eine Zustandsprüfung erstellt haben, müssen Sie die Zustandsprüfung aktualisieren. Weitere Informationen finden Sie unter Aktualisierung der Gesundheitschecks, wenn Sie die CloudWatch Alarmeinstellungen ändern (Zustandsprüfungen, die nur einen CloudWatch Alarm überwachen).

Status der Zustandsprüfung

Wählen Sie den Status der Zustandsprüfung (gesund, fehlerhaft oder letzter bekannter Status), wenn CloudWatch nicht genügend Daten vorliegen, um den Status des Alarms zu bestimmen, den Sie für den CloudWatchAlarm ausgewählt haben. Wenn Sie sich dafür entscheiden, den letzten bekannten Status zu verwenden, verwendet Route 53 den Status der Zustandsprüfung von dem Zeitpunkt, zu dem das letzte Mal genügend Daten zur Verfügung CloudWatch standen, um den Alarmstatus zu bestimmen. Bei neuen Zustandsprüfungen, die keinen letzten bekannten Status haben, ist der Standardstatus für die Zustandsprüfung „fehlerfrei“.

Der Wert Health Check Status bietet einen temporären Status, wenn der Datenstream für eine CloudWatch Metrik kurzzeitig nicht verfügbar ist. (Route 53 überwacht Datenströme auf

CloudWatch Messwerte, nicht auf den Status des entsprechenden Alarms.) Wenn die Metrik häufig oder für lange Zeit (länger als ein paar Stunden) nicht verfügbar ist, empfehlen wir Ihnen, den letzten bekannten Status nicht zu verwenden.

Status der Integritätsprüfung umkehren (nur alte Konsole)

Informationen zum Umkehren einer Systemdiagnose auf der neuen Konsole finden Sie unter. Integritätsprüfungen rückgängig machen

Wählen Sie, ob Sie möchten, dass Route 53 den Status einer Zustandsprüfung umkehrt. Wenn Sie diese Option auswählen, betrachtet Route 53 Zustandsprüfungen als fehlerhaft, wenn sie den Status "fehlerfrei" aufweisen, und umgekehrt.

Deaktiviert (nur alte Konsole)

Informationen zum Deaktivieren einer Systemdiagnose auf der neuen Konsole finden Sie unterGesundheitschecks deaktivieren oder aktivieren.

Stoppt die Ausführung von Zustandsprüfungen durch Route 53. Wenn Sie eine Zustandsprüfung deaktivieren, hört Route 53 auf, die entsprechenden CloudWatch Messwerte zu überwachen.

Nachdem eine Zustandsprüfung deaktiviert wurde, stuft Route 53 den Status der Zustandsprüfung immer als fehlerfrei ein. Wenn Sie ein DNS Failover konfiguriert haben, leitet Route 53 weiterhin Datenverkehr an die entsprechenden Ressourcen weiter. Wenn Sie die Weiterleitung von Datenverkehr zu einer Ressource beenden möchten, kehren Sie die Zustandsprüfung um.

> **Note**
>
> Gebühren für eine Zustandsprüfung gelten weiterhin, auch wenn die Zustandsprüfung deaktiviert ist.

Erweiterte Konfiguration (nur "Monitor an endpoint")

> **Note**
>
> Wir aktualisieren die Health Checks-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

- New console
- Alte Konsole

New console

- Intervall anfordern
- Fehlerschwellenwert
- Abgleich von Zeichenketten
- Suchen Sie nach Zeichenketten
- Latenzdiagramme
- SNI aktivieren
- Host name

Anfrageintervall

Die Anzahl der Sekunden, die zwischen dem Zeitpunkt liegen, wenn jeder Route 53-Zustandsprüfer eine Antwort von Ihrem Endpunkt erhält, und dem Zeitpunkt, wenn er die nächste Anfrage für eine Zustandsprüfung senden. Wenn Sie ein Intervall von 30 Sekunden auswählen, sendet jeder Route 53-Zustandsprüfer in Rechenzentren auf der ganzen Welt Ihrem Endpunkt alle 30 Sekunden eine Anforderung für eine Zustandsprüfung. Ihr Endpunkt wird durchschnittlich alle zwei Sekunden eine Anforderung für eine Zustandsprüfung erhalten. Wenn Sie ein Intervall von 10 Sekunden auswählen, erhält der Endpunkt mehr als einmal pro Sekunde eine Anforderung.

Beachten Sie, dass Route 53-Zustandsprüfer in verschiedenen Rechenzentren nicht miteinander koordinieren, sodass Sie manchmal mehrere Anfragen pro Sekunde sehen, unabhängig des von Ihnen gewählten Intervalls, gefolgt von wenigen Sekunden ohne Zustandsprüfungen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Request interval nicht mehr ändern.

> **Note**
>
> Wenn Sie Fast (10 seconds) für den Wert von Request interval auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

Fehlerschwellenwert

Die Anzahl der aufeinanderfolgenden Integritätsprüfungen, die ein Endpunkt bestehen oder nicht bestehen muss, damit Route 53 den aktuellen Status des Endpunkts von fehlerhaft in fehlerfrei oder umgekehrt ändert. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Zeichenfolgenabgleich (nur HTTP und HTTPS)

Ob Sie möchten, dass Route 53 den Zustand eines Endpunkts bestimmt, indem er eine HTTP- oder HTTPS-Anforderung an den Endpunkt sendet und den Antworttext nach einer angegebenen Zeichenfolge durchsucht. Wenn der Antworttext den Wert enthält, den Sie unter Search string angegeben haben, betrachtet Route 53 den Endpunkt als fehlerfrei. Wenn dies nicht der Fall ist, oder wenn der Endpunkt nicht reagiert, betrachtet Route 53 den Endpunkt als fehlerhaft. Die Suchzeichenfolge muss vollständig in den ersten 5.120 Bytes des Antworttexts erscheinen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von String matching nicht mehr ändern.

> **Note**
>
> Wenn Sie Yes für den Wert von String matching auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

Wie Health Checkers mit einer komprimierten Antwort umgehen

Wenn es sich bei dem Endpunkt um einen Webserver handelt, der eine komprimierte Antwort zurückgibt, dekomprimiert die Route 53-Integritätsprüfung die Antwort, bevor die angegebene Suchzeichenfolge überprüft wird, nur dann, wenn der Webserver die Antwort mit einem Komprimierungsalgorithmus komprimiert hat, den Integritätsprüfer unterstützen. Health Checkers unterstützen die folgenden Komprimierungsalgorithmen:

- Gzip
- DEFLATE

Wenn die Antwort mit einem anderen Algorithmus komprimiert wird, kann die Integritätsprüfung die Antwort nicht dekomprimieren, bevor sie nach der Zeichenfolge sucht. In diesem Fall schlägt die Suche fast immer fehl, und Route 53 betrachtet den Endpunkt als fehlerhaft

Suchzeichenfolge (nur wenn "String matching" aktiviert ist)

Die Zeichenfolge, nach der Route 53 im Text der Antwort Ihres Endpunkts suchen soll. Die maximale Länge beträgt 255 Zeichen.

Bei der Suche nach Search string im Antworttext beachtet Route 53 Groß- und Kleinschreibung.

Latenzdiagramme

Wählen Sie aus, ob Route 53 die Latenz zwischen Health Checks in mehreren AWS Regionen und Ihrem Endpunkt messen soll. Wenn Sie diese Option wählen, werden CloudWatch Latenzdiagramme auf der Registerkarte Latenz auf der Seite Integritätsprüfungen in der Route 53-Konsole angezeigt. Wenn Route 53-Zustandsprüfer keine Verbindung mit dem Endpunkt herstellen können, kann Route 53 keine Latenzdiagramme für den jeweiligen Endpunkt anzeigen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Latency measurements nicht mehr ändern.

> **Note**
>
> Wenn Sie Route 53 konfigurieren, um die Latenz zwischen Zustandsprüfern und Ihrem Endpunkt zu messen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

SNI aktivieren (nur HTTPS)

Geben Sie an, ob Route 53 während der TLS-Aushandlung den Hostnamen zum Endpunkt in der Nachricht `client_hello` senden soll. Dadurch kann der Endpunkt auf die HTTPS-Anfrage mit dem entsprechenden SSL/TLS Zertifikat antworten.

Einige Endpunkte erfordern, dass HTTPS-Anfragen den Hostnamen in der client_hello-Nachricht enthalten. Wenn Sie SNI nicht aktivieren, wird bei der Integritätsprüfung

möglicherweise ein Fehler angezeigt. Die Fehlermeldung hängt davon ab, wie der Server so konfiguriert ist, dass er die Anfrage beantwortet, die keine SNI-Informationen enthält. Eine Integritätsprüfung kann auch aus anderen Gründen den Status „Fehlgeschlagen“ haben. Wenn SNI aktiviert ist und Sie weiterhin den Fehler erhalten, prüfen Sie die SSL-/TLS-Konfiguration auf dem Endpunkt und vergewissern Sie sich, dass Ihr Zertifikat gültig ist.

Beachten Sie die folgenden Voraussetzungen:

- Der Endpunkt muss SNI unterstützen.
- Das SSL/TLS Zertifikat auf Ihrem Endpunkt enthält einen Domainnamen im `Common Name` Feld und möglicherweise mehrere weitere in dem `Subject Alternative Names` Feld. Einer der Domänennamen im Zertifikat muss mit dem Wert übereinstimmen, den Sie für Host name angeben.

Zustandsprüferregionen

Wählen Sie, ob Route 53 den Zustand des Endpunkts mithilfe von Zustandsprüfern in den empfohlenen Regionen oder mithilfe von Zustandsprüfungen in Regionen, die Sie angeben, überprüfen soll.

Wenn Sie eine Statusprüfung aktualisieren, damit eine Region entfernt wird, aus der Statusprüfungen durchgeführt hat, führt Route 53 bis zu einer Stunde weiterhin Prüfungen aus dieser Region durch. Auf diese Weise wird sichergestellt, dass einige Statusprüfer den Endpunkt immer überprüfen (z. B. wenn Sie drei Regionen durch vier verschiedenen Regionen ersetzen).

Wenn Sie Customize wählen, wählen Sie das x aus, um eine Region zu entfernen. Klicken Sie auf den Bereich unten in der Liste, um eine Region erneut zur Liste hinzuzufügen. Sie müssen mindestens drei Regionen angeben.

Host-Name (nur "Specify endpoint by IP address", nur HTTP- und HTTPS-Protokolle)

Der Wert, den Route 53 in der `Host`-Kopfzeile in HTTP- und HTTPS-Zustandsprüfungen angeben soll. Dies ist in der Regel der vollqualifizierte DNS-Name der Website, auf der Route 53 Zustandsprüfungen durchführen soll. Wenn Route 53 den Zustand eines Endpunkts überprüft, erstellt es den `Host`-Header folgendermaßen:

- Wenn Sie einen Wert von **`80`** für Port und von HTTP für Protocol festlegen, übergibt Route 53 an den Endpunkt eine `Host`-Kopfzeile, die den Wert Host name enthält.
- Wenn Sie den Wert **`443`** für Port und HTdTPS für Protokoll angeben, leitet Route 53 einen `Host` Header an den Endpunkt weiter, der den Wert des Hostnamens enthält.

- Wenn Sie einen anderen Wert für Port und entweder HTTP oder HTTPS für Protokoll angeben, leitet Route 53 einen `Host` Header an den Endpunkt weiter, der den Wert enthält *`Host name`*:*`Port`*.

Wenn Sie sich dafür entscheiden, den Endpunkt durch die IP-Adresse anzugeben, und Sie keinen Wert für Host name festlegen, ersetzt Route 53 IP address in der -`Host`Kopfzeile in allen vorangegangenen Fällen.

Old console

Wenn Sie die Option für die Überwachung eines Endpunkts auswählen, können Sie auch die folgenden Einstellungen festlegen:

- Anforderungsintervall
- Fehlerschwellenwert
- Abgleich von Zeichenketten
- Zeichenfolge suchen
- Latenzdiagramm
- SNI aktivieren
- Health Checker Regionen
- Status der Zustandsprüfung umkehren
- Disabled

Anfrageintervall

Die Anzahl der Sekunden, die zwischen dem Zeitpunkt liegen, wenn jeder Route 53-Zustandsprüfer eine Antwort von Ihrem Endpunkt erhält, und dem Zeitpunkt, wenn er die nächste Anfrage für eine Zustandsprüfung senden. Wenn Sie ein Intervall von 30 Sekunden auswählen, sendet jeder Route 53-Zustandsprüfer in Rechenzentren auf der ganzen Welt Ihrem Endpunkt alle 30 Sekunden eine Anforderung für eine Zustandsprüfung. Ihr Endpunkt wird durchschnittlich alle zwei Sekunden eine Anforderung für eine Zustandsprüfung erhalten. Wenn Sie ein Intervall von 10 Sekunden auswählen, erhält der Endpunkt mehr als einmal pro Sekunde eine Anforderung.

Beachten Sie, dass Route 53-Zustandsprüfer in verschiedenen Rechenzentren nicht miteinander koordinieren, sodass Sie manchmal mehrere Anfragen pro Sekunde sehen,

unabhängig des von Ihnen gewählten Intervalls, gefolgt von wenigen Sekunden ohne Zustandsprüfungen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Request interval nicht mehr ändern.

> **Note**
>
> Wenn Sie Fast (10 seconds) für den Wert von Request interval auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

Fehlerschwellenwert

Die Anzahl der aufeinanderfolgenden Integritätsprüfungen, die ein Endpunkt bestehen oder nicht bestehen muss, damit Route 53 den aktuellen Status des Endpunkts von fehlerhaft in fehlerfrei oder umgekehrt ändert. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Zeichenfolgenabgleich (nur HTTP und HTTPS)

Ob Sie möchten, dass Route 53 den Zustand eines Endpunkts bestimmt, indem er eine HTTP- oder HTTPS-Anforderung an den Endpunkt sendet und den Antworttext nach einer angegebenen Zeichenfolge durchsucht. Wenn der Antworttext den Wert enthält, den Sie unter Search string angegeben haben, betrachtet Route 53 den Endpunkt als fehlerfrei. Wenn dies nicht der Fall ist, oder wenn der Endpunkt nicht reagiert, betrachtet Route 53 den Endpunkt als fehlerhaft. Die Suchzeichenfolge muss vollständig in den ersten 5.120 Bytes des Antworttexts erscheinen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von String matching nicht mehr ändern.

> **Note**
>
> Wenn Sie Yes für den Wert von String matching auswählen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

Wie Health Checkers mit einer komprimierten Antwort umgehen

Wenn es sich bei dem Endpunkt um einen Webserver handelt, der eine komprimierte Antwort zurückgibt, dekomprimiert die Route 53-Integritätsprüfung die Antwort, bevor die angegebene Suchzeichenfolge überprüft wird, nur dann, wenn der Webserver die Antwort mit einem Komprimierungsalgorithmus komprimiert hat, den Integritätsprüfer unterstützen. Health Checkers unterstützen die folgenden Komprimierungsalgorithmen:

- Gzip
- DEFLATE

Wenn die Antwort mit einem anderen Algorithmus komprimiert wird, kann die Integritätsprüfung die Antwort nicht dekomprimieren, bevor sie nach der Zeichenfolge sucht. In diesem Fall schlägt die Suche fast immer fehl, und Route 53 betrachtet den Endpunkt als fehlerhaft

Suchzeichenfolge (nur wenn "String matching" aktiviert ist)

Die Zeichenfolge, nach der Route 53 im Text der Antwort Ihres Endpunkts suchen soll. Die maximale Länge beträgt 255 Zeichen.

Bei der Suche nach Search string im Antworttext beachtet Route 53 Groß- und Kleinschreibung.

Latenzdiagramme

Wählen Sie aus, ob Route 53 die Latenz zwischen Health Checks in mehreren AWS Regionen und Ihrem Endpunkt messen soll. Wenn Sie diese Option wählen, werden CloudWatch Latenzdiagramme auf der Registerkarte Latenz auf der Seite Integritätsprüfungen in der Route 53-Konsole angezeigt. Wenn Route 53-Zustandsprüfer keine Verbindung mit dem Endpunkt herstellen können, kann Route 53 keine Latenzdiagramme für den jeweiligen Endpunkt anzeigen.

Nachdem Sie eine Zustandsprüfung erstellt haben, können Sie den Wert von Latency measurements nicht mehr ändern.

> **Note**
>
> Wenn Sie Route 53 konfigurieren, um die Latenz zwischen Zustandsprüfern und Ihrem Endpunkt zu messen, fällt eine zusätzliche Gebühr an. Weitere Informationen dazu finden Sie unter Route 53 – Preise.

SNI aktivieren (nur HTTPS)

Geben Sie an, ob Route 53 während der TLS-Aushandlung den Hostnamen zum Endpunkt in der Nachricht `client_hello` senden soll. Dadurch kann der Endpunkt auf die HTTPS-Anfrage mit dem entsprechenden SSL/TLS Zertifikat antworten.

Einige Endpunkte verlangen, dass HTTPS-Anforderungen den Hostnamen in die Nachricht `client_hello` einfügen. Wenn Sie SNI nicht aktivieren, wird bei der Integritätsprüfung möglicherweise ein Fehler angezeigt. Die Fehlermeldung hängt davon ab, wie der Server so konfiguriert ist, dass er die Anfrage beantwortet, die keine SNI-Informationen enthält. Eine Integritätsprüfung kann auch aus anderen Gründen den Status „Fehlgeschlagen“ haben. Wenn SNI aktiviert ist und der Fehler weiterhin angezeigt wird, überprüfen Sie die SSL/TLS Konfiguration auf Ihrem Endpunkt und stellen Sie sicher, dass Ihr Zertifikat gültig ist.

Beachten Sie die folgenden Voraussetzungen:

- Der Endpunkt muss SNI unterstützen.
- Das SSL/TLS Zertifikat auf Ihrem Endpunkt enthält einen Domainnamen im `Common Name` Feld und möglicherweise mehrere weitere in dem `Subject Alternative Names` Feld. Einer der Domänennamen im Zertifikat muss mit dem Wert übereinstimmen, den Sie für Host name angeben.

Zustandsprüferregionen

Wählen Sie, ob Route 53 den Zustand des Endpunkts mithilfe von Zustandsprüfern in den empfohlenen Regionen oder mithilfe von Zustandsprüfungen in Regionen, die Sie angeben, überprüfen soll.

Wenn Sie eine Statusprüfung aktualisieren, damit eine Region entfernt wird, aus der Statusprüfungen durchgeführt hat, führt Route 53 bis zu einer Stunde weiterhin Prüfungen aus dieser Region durch. Auf diese Weise wird sichergestellt, dass einige Statusprüfer den Endpunkt immer überprüfen (z. B. wenn Sie drei Regionen durch vier verschiedenen Regionen ersetzen).

Wenn Sie Customize wählen, wählen Sie das x aus, um eine Region zu entfernen. Klicken Sie auf den Bereich unten in der Liste, um eine Region erneut zur Liste hinzuzufügen. Sie müssen mindestens drei Regionen angeben.

Status der Integritätsprüfung umkehren (nur alte Konsole)

Informationen zum Umkehren einer Systemdiagnose auf der neuen Konsole finden Sie unter. Integritätsprüfungen rückgängig machen

Wählen Sie, ob Sie möchten, dass Route 53 den Status einer Zustandsprüfung umkehrt. Wenn Sie diese Option wählen, betrachtet Route 53 eine Zustandsprüfung als fehlerhaft, wenn der Status fehlerfrei ist, und umgekehrt. Beispielsweise wollen Sie vielleicht, dass Route 53 eine Zustandsprüfung als fehlerhaft einstuft, wenn Sie einen Zeichenfolgenabgleich konfigurieren und der Endpunkt einen festgelegten Wert zurückgibt.

Deaktiviert (nur alte Konsole)

Informationen zum Deaktivieren einer Systemdiagnose auf der neuen Konsole finden Sie unterGesundheitschecks deaktivieren oder aktivieren.

Stoppt die Ausführung von Zustandsprüfungen durch Route 53. Wenn Sie eine Zustandsprüfung deaktivieren, versucht Route 53 nicht mehr, eine TCP-Verbindung mit dem Endpunkt herzustellen.

Nachdem eine Zustandsprüfung deaktiviert wurde, stuft Route 53 den Status der Zustandsprüfung immer als fehlerfrei ein. Wenn Sie ein DNS Failover konfiguriert haben, leitet Route 53 weiterhin Datenverkehr an die entsprechenden Ressourcen weiter. Wenn Sie die Weiterleitung von Datenverkehr zu einer Ressource beenden möchten, kehren Sie die Zustandsprüfung um.

> **Note**
>
> Gebühren für eine Zustandsprüfung gelten weiterhin, auch wenn die Zustandsprüfung deaktiviert ist.

Eine Benachrichtigung erhalten, wenn eine Zustandsprüfung fehlschlägt

Verwenden Sie die folgenden Optionen zum Konfigurieren von E-Mail-Benachrichtigungen, wenn eine Zustandsprüfung fehlschlägt:

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Alarm erstellen (nur beim Erstellen von Zustandsprüfungen)

Geben Sie an, ob Sie einen CloudWatch Standardalarm erstellen möchten. Wenn Sie Ja wählen, wird Ihnen eine Amazon SNS SNS-Benachrichtigung CloudWatch gesendet, wenn sich der Status dieses Endpunkts auf ungesund ändert und Route 53 den Endpunkt für eine Minute als fehlerhaft einstuft.

> **Note**
>
> Wenn Sie Ihnen eine weitere Amazon SNS SNS-Benachrichtigung senden möchten CloudWatch , wenn der Status wieder fehlerfrei ist, können Sie nach dem Erstellen der Zustandsprüfung einen weiteren Alarm erstellen. Weitere Informationen finden Sie unter CloudWatch Amazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie einen Alarm für eine vorhandene Zustandsprüfung einrichten oder benachrichtigt werden möchten, wenn Route 53 den Endpunkt für mehr oder weniger als eine Minute (Standardwert) als fehlerhaft ansieht, wählen Sie No aus und fügen Sie einen Alarm hinzu, nachdem Sie die Zustandsprüfung erstellt haben. Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

Benachrichtigung senden an (nur beim Erstellen eines Alarms)

Geben Sie an CloudWatch , ob Sie Benachrichtigungen zu einem bestehenden Amazon SNS SNS-Thema oder zu einem neuen senden möchten:

- Existing SNS topic - Wählen Sie den Namen des Themas aus der Liste aus. Die Lambda-Funktion muss sich in der Region USA Ost (Nord-Virginia) befinden.
- New SNS topic - Geben Sie einen Namen für das Thema unter Topic name ein und geben Sie unter Recipients die E-Mail-Adressen an, denen Sie Benachrichtigungen senden möchten. Trennen Sie mehrere Adressen durch Kommas (,), Strichpunkte (;) oder Leerzeichen.

  Die Route 53 erstellt das Thema in der Region USA Ost (Nord-Virginia).

Themenname (nur beim Erstellen eines neuen SNS-Themas)

Wenn Sie New SNS Topic angegeben haben, geben Sie den Namen des neuen Themas ein.

Empfänger-E-Mail-Adressen (nur beim Erstellen eines neuen SNS-Themas)

Wenn Sie New SNS topic angegeben haben, geben Sie die E-Mail-Adressen an, an die Benachrichtigungen gesendet werden sollen. Trennen Sie mehrere Namen durch Kommas (,), Strichpunkte (;) oder Leerzeichen.

Werte, die Amazon Route 53 anzeigt, wenn Sie eine Zustandsprüfung erstellen

Die Seite Create Health Check zeigt die folgenden Werte basierend auf den Werten an, die Sie eingegeben haben:

URL

Entweder die vollständige URL (für HTTP- oder HTTPS-Zustandsprüfungen) oder die IP-Adresse und den Port (für TCP-Zustandsprüfungen), an die Route 53 bei der Durchführung von Zustandsprüfungen Anfragen sendet.

Art der Zustandsprüfung

Entweder Basic oder Basic + additional options, basierend auf den Einstellungen, die Sie für diese Zustandsprüfung angegeben haben. Weitere Informationen zu den Preisen für die zusätzlichen Optionen finden Sie unter Route 53 – Preise.

Aktualisierung der Gesundheitschecks, wenn Sie die CloudWatch Alarmeinstellungen ändern (Zustandsprüfungen, die nur einen CloudWatch Alarm überwachen)

Wenn Sie eine Route 53-Zustandsprüfung erstellen, die den Datenstrom auf einen CloudWatch Alarm überwacht, und dann die Einstellungen im CloudWatch Alarm aktualisieren, aktualisiert Route 53 die Alarmeinstellungen in der Zustandsprüfung nicht automatisch. Wenn Sie möchten, dass die Zustandsprüfung die neuen Alarmeinstellungen verwendet, müssen Sie die Zustandsprüfung aktualisieren.

> **Note**
>
> Um eine Zustandsprüfung programmgesteuert zu aktualisieren, können Sie die API `UpdateHealthCheck` verwenden. Geben Sie einfach die aktuellen Werte für

`AlarmIdentifier` und an`Region`, und Route 53 erhält die neuesten Einstellungen von CloudWatch. Weitere Informationen finden Sie UpdateHealthCheckin der Amazon Route 53 API-Referenz.

> **Note**
>
> Wir aktualisieren die Health Checks Console für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Um einen Gesundheitscheck mit neuen CloudWatch Alarmeinstellungen zu aktualisieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID für die Zustandsprüfung aus, die Sie aktualisieren möchten.
4. Wählen Sie Bearbeiten aus.

   In einem Hinweis wird erklärt, dass sich der CloudWatch Alarm für den Gesundheitscheck geändert hat. Das Feld Details zeigt die neuen Alarmeinstellungen.
5. Wählen Sie Speichern.

Old console

Um einen Gesundheitscheck mit neuen CloudWatch Alarmeinstellungen zu aktualisieren (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Aktivieren Sie das Kontrollkästchen für die Zustandsprüfung, die Sie aktualisieren möchten.
4. Wählen Sie Edit health check aus.

   In einem Hinweis wird erklärt, dass sich der CloudWatch Alarm für den Gesundheitscheck geändert hat. Das Feld Details zeigt die neuen Alarmeinstellungen.
5. Wählen Sie Speichern.

Gesundheitschecks deaktivieren oder aktivieren

Durch das Deaktivieren einer Integritätsprüfung kann Route 53 keine Integritätsprüfungen mehr durchführen. Wenn Sie eine Zustandsprüfung deaktivieren, wird die Aggregation des Status der referenzierten Zustandsprüfungen durch Route 53 gestoppt. Nachdem eine Zustandsprüfung deaktiviert wurde, stuft Route 53 den Status der Zustandsprüfung immer als fehlerfrei ein. Wenn Sie ein DNS Failover konfiguriert haben, leitet Route 53 weiterhin Datenverkehr an die entsprechenden Ressourcen weiter. Wenn Sie die Weiterleitung von Datenverkehr zu einer Ressource beenden möchten, ändern Sie den Wert von Inverted.

> **Note**
>
> Wir aktualisieren die Health Checks-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Sie können eine Zustandsprüfung auf der alten Konsole deaktivieren oder aktivieren, wenn Sie die Zustandsprüfung erstellen oder bearbeiten. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.

Gehen Sie wie folgt vor, um die Integritätsprüfungen auf der neuen Konsole zu deaktivieren.

Um eine Systemdiagnose zu deaktivieren oder zu aktivieren (nur neue Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie in der Spalte Aktionen die drei Punkte und dann Deaktivieren oder Aktivieren aus.

Oder wählen Sie die verknüpfte ID der Zustandsprüfung aus, die Sie deaktivieren oder aktivieren möchten.

4. In der Konfigurationstabelle gibt das Feld Status an, ob die Integritätsprüfung aktiviert oder deaktiviert ist.
5. Wählen Sie Deaktivieren oder Aktivieren, um die Integritätsprüfung entweder zu deaktivieren oder zu aktivieren.

Integritätsprüfungen rückgängig machen

Wenn Sie eine Zustandsprüfung umkehren, betrachtet Route 53 die Zustandsprüfung als fehlerhaft, wenn der Status fehlerfrei ist, und umgekehrt.

> **Note**
>
> Wir aktualisieren die Konsole für Zustandsprüfungen für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Sie können eine Zustandsprüfung auf der alten Konsole rückgängig machen, wenn Sie die Zustandsprüfung erstellen oder bearbeiten. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.

Gehen Sie wie folgt vor, um Integritätsprüfungen auf der neuen Konsole umzukehren.

Um eine Integritätsprüfung umzukehren (nur auf der neuen Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie in der Spalte Aktionen die drei Punkte aus und klicken Sie dann auf Umkehren.

   Oder — Wählen Sie die verknüpfte ID der Zustandsprüfung aus, die Sie rückgängig machen möchten.
4. In der Konfigurationstabelle gibt das Feld Invertiert an, ob die Integritätsprüfung invertiert (Ja) oder nicht (Nein) ist.
5. Wählen Sie Invertieren, um die Integritätsprüfung umzukehren.

Wenn Sie den umgekehrten Status rückgängig machen möchten und das Feld Invertiert den Wert Ja hat, wählen Sie erneut „Invertieren“.

Löschen von Zustandsprüfungen

Gehen Sie wie folgt vor, um Integritätsprüfungen zu deaktivieren.

> **Note**
>
> Wenn Sie bei der Registrierung einer Instanz eine Route 53-Zustandsprüfung verwenden AWS Cloud Map und für deren Erstellung konfiguriert AWS Cloud Map haben, können Sie die Route 53-Konsole nicht verwenden, um die Zustandsprüfung zu löschen. Die Zustandsprüfung wird automatisch gelöscht, wenn Sie die Instance abmelden. Es kann mehrere Stunden dauern, bis die Zustandsprüfung nicht mehr in der Route 53-Konsole angezeigt wird.

> **Note**
>
> Wir aktualisieren die Konsole für die Zustandsprüfungen für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Um eine Zustandsprüfung zu löschen

1. Wenn Sie Zustandsprüfungen löschen, die im Zusammenhang mit Datensätzen stehen, führen Sie die empfohlenen Aufgaben in Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover aus.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

3. Wählen Sie im Navigationsbereich Health Checks aus.
4. Wählen Sie die verknüpfte ID der Zustandsprüfung aus, die Sie löschen möchten.
5. Wählen Sie Löschen aus.
6. Geben Sie den Text **`confirm`** in das Textfeld ein und wählen Sie dann Löschen.

Old console

So löschen Sie eine Zustandsprüfung (Konsole)

1. Wenn Sie Zustandsprüfungen löschen, die im Zusammenhang mit Datensätzen stehen, führen Sie die empfohlenen Aufgaben in Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover aus.
2. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
3. Wählen Sie im Navigationsbereich Health Checks aus.
4. Wählen Sie im rechten Bereich die Zustandsprüfung aus, die Sie löschen möchten.
5. Wählen Sie Delete Health Check.
6. Wählen Sie zur Bestätigung Yes, Delete.

Aktualisieren oder Löschen von Zustandsprüfungen bei konfiguriertem DNS Failover

Wenn Sie Zustandsprüfungen aktualisieren oder löschen möchten, die mit Datensätzen in Verbindung stehen, oder wenn Sie Datensätze ändern möchten, die mit Zustandsprüfungen im Zusammenhang stehen, müssen Sie die Auswirkungen Ihrer Änderungen auf die Weiterleitung von DNS-Abfragen und Ihre DNS-Failover-Konfiguration berücksichtigen.

> **Important**
>
> Route 53 hindert Sie nicht am Löschen einer Zustandsprüfung, auch wenn die Zustandsprüfung einem oder mehreren Datensätzen zugeordnet ist. Wenn Sie eine Zustandsprüfung löschen, ohne die zugehörigen Datensätze zu aktualisieren, kann der zukünftige Status der Zustandsprüfung nicht vorhergesehen werden und könnte sich

verändern. Dies wirkt sich auf das Routing von DNS-Abfragen für Ihre DNS Failover-Konfiguration aus.

Wenn Sie Zustandsprüfungen aktualisieren oder löschen möchten, die bereits mit Datensätzen verknüpft sind, empfehlen wir Ihnen, die folgenden Aufgaben auszuführen:

1. Identifizieren Sie die Datensätze, die mit den Zustandsprüfungen verknüpft sind. Um die Datensätze zu identifizieren, die mit einer Zustandsprüfung verknüpft sind, müssen Sie einen der folgenden Schritte ausführen:

   - Überprüfen Sie die Datensätze in jeder gehosteten Zone mittels der Route 53-Konsole. Weitere Informationen finden Sie unter Auflisten von Datensätzen.
   - Führen Sie die API-Aktion `ListResourceRecordSets` für jede gehostete Zone aus und überprüfen Sie die Antwort. Weitere Informationen finden Sie ListResourceRecordSetsin der Amazon Route 53 API-Referenz.
2. Bewerten Sie die Änderung des Verhaltens, die sich aus der Aktualisierung oder Löschung von Zustandsprüfungen oder aus der Aktualisierung von Datensätzen ergibt. Bestimmen Sie anhand dieser Bewertung, welche Änderungen vorgenommen werden sollen.

   Weitere Informationen finden Sie unter Was geschieht, wenn Sie Zustandsprüfungen überspringen?
3. Ändern Sie Zustandsprüfungen und Datensätze wie zutreffend. Weitere Informationen finden Sie unter den folgenden Themen:

   - Erstellen und Aktualisieren von Zustandsprüfungen
   - Bearbeiten von Datensätzen
4. Löschen Sie die Zustandsprüfungen, die Sie nicht länger verwenden (sofern vorhanden). Weitere Informationen finden Sie unter Löschen von Zustandsprüfungen.

Konfigurieren von Router- und Firewall-Regeln für Amazon Route 53-Zustandsprüfungen

Wenn Route 53 den Zustand eines Endpunkts überprüft, sendet sie eine HTTP-, HTTPS- oder TCP-Anforderung an die IP-Adresse und den Port, die Sie beim Erstellen der Zustandsprüfung angegeben

haben. Für eine erfolgreiche Zustandsprüfung müssen Ihre Router- und Firewall-Regeln eingehenden Datenverkehr von den IP-Adressen zulassen, die die -Zustandsprüfer verwenden.

Die aktuelle Liste der IP-Adressen für Route 53-Integritätsprüfungen, für Route 53-Nameserver und für andere AWS Dienste finden Sie unterIP-Adressbereiche von Amazon Route 53-Servern.

Bei Amazon EC2 fungieren Sicherheitsgruppen als Firewalls. Weitere Informationen finden Sie unter EC2 Amazon-Sicherheitsgruppen im EC2 Amazon-Benutzerhandbuch. Um Ihre Sicherheitsgruppen so zu konfigurieren, dass sie Route 53-Zustandsprüfungen zulassen, können Sie entweder eingehenden Verkehr aus jedem IP-Adressbereich zulassen oder eine AWS-verwaltete Präfixliste verwenden.

Um die Präfixliste AWS-managed zu verwenden, ändern Sie Ihre Sicherheitsgruppe so`com.amazonaws.<region>.route53-healthchecks`, dass eingehender Datenverkehr AWS-Region von Ihrer EC2 Amazon-Instance oder -Ressource zugelassen `<region>` wird. Wenn Sie Route 53-Zustandsprüfungen zur Überprüfung von IPv6 Endpunkten verwenden, sollten Sie auch eingehenden Datenverkehr von zulassen. `com.amazonaws.<region>.ipv6.route53-healthchecks`

Weitere Informationen zu AWS-verwalteten Präfixlisten finden Sie unter Arbeiten mit AWS-verwalteten Präfixlisten im Amazon VPC-Benutzerhandbuch.

> **Important**
>
> Wenn Sie IP-Adressen zu einer Liste zulässiger IP-Adressen hinzufügen, fügen Sie alle IP-Adressen im CIDR-Bereich für jede AWS Region hinzu, die Sie bei der Erstellung von Integritätsprüfungen angegeben haben, sowie den globalen CIDR-Bereich. Sie können sehen, dass Anforderungen für Statusprüfungen aus einer IP-Adresse in einer Region stammen. Allerdings kann sich die IP-Adresse jederzeit in eine andere IP-Adresse für diese Region ändern.
>
> Wenn Sie sicherstellen möchten, dass sowohl die aktuelle als auch die ältere IP-Adresse der Zustandsprüfung enthalten, fügen Sie ALLE IP-Adressbereiche /26 und /18 zur Zulassungsliste hinzu. Eine vollständige Liste finden Sie unter AWS -IP-Adressbereiche in der Allgemeine AWS-Referenz.
>
> Wenn Sie Ihrer Sicherheitsgruppe für eingehende Nachrichten die Liste mit AWS verwaltetem Präfix hinzufügen, werden automatisch alle erforderlichen Bereiche hinzugefügt.

Konfigurieren von DNS Failover

Wenn Sie mehr als eine Ressource mit der gleichen Funktion haben, z. B. mehr als einen HTTP- oder E-Mail-Server, können Sie Amazon Route 53 so konfigurieren, dass der Zustand Ihrer Ressourcen überprüft und auf DNS-Abfragen nur mit fehlerfreien Ressourcen reagiert wird. Nehmen wir beispielsweise an, dass die Website „example.com“ auf sechs Servern gehostet wird, von denen sich jeweils zwei in drei Rechenzentren irgendwo auf der Welt befinden. Sie können Route 53 so konfigurieren, dass er die Zustände dieser Server prüft und auf DNS-Abfragen für „example.com“ nur mit den derzeit fehlerfreien Servern antwortet.

Route 53 kann den Zustand der Ressourcen in einfachen und komplexen Konfigurationen prüfen:

- In einfachen Konfigurationen erstellen Sie für „example.com“ eine Gruppe von Datensätzen mit demselben Namen und Typ, z. B. eine Gruppe von gewichteten Datensätzen mit dem Typ A. Anschließend konfigurieren Sie Route 53 zum Überprüfen des Zustands der entsprechenden Ressourcen. Route 53 beantwortet DNS-Abfragen basierend auf dem Zustand der Ressourcen. Weitere Informationen finden Sie unter So funktionieren Zustandsprüfungen in einfachen Amazon Route 53-Konfigurationen.
- In komplexeren Konfigurationen erstellen Sie eine Struktur von Datensätzen, mit denen der Datenverkehr nach mehreren Kriterien weitergeleitet wird. Wenn beispielsweise die Latenz für Ihre Benutzer Ihr wichtigstes Kriterium ist, können Sie Latenz-Aliasdatensätze verwenden, um den Datenverkehr zu der Region weiterzuleiten, die die beste Latenz bietet. Die Latenz-Aliasdatensätze können in jeder Region gewichtete Datensätze als Aliasziel haben. Die gewichteten Datensätze können den Datenverkehr je nach Instance-Typ an EC2 Instances weiterleiten. Wie bei einer einfachen Konfiguration können Sie Route 53 so konfigurieren, dass der Datenverkehr basierend auf dem Zustand Ihrer Ressourcen weitergeleitet wird. Weitere Informationen finden Sie unter So funktionieren Zustandsprüfungen in komplexen Amazon-Route-53-Konfigurationen.

Themen

- So vermeidet Amazon Route 53 Failover-Probleme

Aufgabenliste für die Konfiguration von DNS Failover

Wenn Sie DNS Failover mit Route 53 konfigurieren möchten, gehen Sie wie folgt vor:

1. Entwerfen Sie ein vollständiges Baumdiagramm Ihrer Konfiguration und geben Sie an, welche Art von Datensatz Sie für die einzelnen Knoten erstellen möchten (gewichteter Alias, Failover, Latenz usw.). Geben Sie oben im Baum die Datensätze für den Domänennamen an, z. B. example.com, den Ihre Benutzer verwenden, um auf Ihre Website oder Webanwendung zu zugreifen.

   Die Arten von Datensätzen, die in Ihrem Baumdiagramm angezeigt werden, hängen von der Komplexität der Konfiguration ab:

   - In einer einfachen Konfiguration enthält Ihr Diagramm entweder keine Aliasdatensätze, oder die Aliasdatensätze leiten Datenverkehr anstatt zu einem anderen Route 53-Datensatz direkt zu einer Ressource weiter, z. B. einem ELB-Load Balancer. Weitere Informationen finden Sie unter So funktionieren Zustandsprüfungen in einfachen Amazon Route 53-Konfigurationen.
   - In einer komplexen Konfiguration enthält das Diagramm eine Kombination aus Aliasdatensätzen (z. B. gewichtete Alias- und Failover-Aliasdatensätze) und Nicht-Aliasdatensätzen in einer Struktur mit mehreren Ebenen wie in den Beispielen im Thema So funktionieren Zustandsprüfungen in komplexen Amazon-Route-53-Konfigurationen gezeigt.

   > **Note**
   >
   > Um schnell und einfach Datensätze für komplexe Weiterleitungskonfigurationen zu erstellen und die Datensätze mit Zustandsprüfungen zu verknüpfen, können Sie den visuellen Datenverkehrs-Editor verwenden und die Konfiguration als Datenverkehrsrichtlinie speichern. Sie können dann die Datenverkehrsrichtlinie mit einem oder mehreren Domainnamen (z. B. example.com) oder Subdomainnamen (z. B. www.example.com) in derselben gehosteten Zone oder in mehreren gehosteten Zonen verknüpfen. Außerdem können Sie ein Rollback der Aktualisierungen durchführen, wenn die neue Konfiguration sich nicht wie erwartet verhält. Weitere Informationen finden Sie unter Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr.

Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Auswählen einer Routing-Richtlinie
- Wählen zwischen Alias- und Nicht-Alias-Datensätzen

2. Erstellen Sie Zustandsprüfungen für die Ressourcen, für die Sie keine Aliaseinträge erstellen können, z. B. EC2 Amazon-Server und E-Mail-Server, die in Ihrem Rechenzentrum laufen. Sie können diese Zustandsprüfungen mit den Nicht-Aliasdatensätzen verknüpfen.

   Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

3. Konfigurieren Sie Router- und Firewall-Regeln nötigenfalls so, dass Route 53 regelmäßige Abfragen an die Endpunkte senden kann, die Sie in Ihren Zustandsprüfungen angegeben haben. Weitere Informationen finden Sie unter Konfigurieren von Router- und Firewall-Regeln für Amazon Route 53-Zustandsprüfungen.

4. Erstellen Sie alle Nicht-Aliasdatensätze im Diagramm und verknüpfen Sie die Zustandsprüfungen, die Sie in Schritt 2 erstellt haben, mit den entsprechenden Datensätzen.

   Wenn Sie DNS Failover in einer Konfiguration konfigurieren, die keine Aliasdatensätze enthält, überspringen Sie die verbleibenden Aufgaben.

5. Erstellen Sie die Aliaseinträge, die den Datenverkehr an AWS Ressourcen weiterleiten, z. B. an ELB-Loadbalancer und CloudFront -Verteilungen. Wenn Route 53 einen anderen Zweig der Struktur verwenden soll, wenn eine Ressource fehlerhaft ist, legen Sie den Wert von Evaluate Target Health für alle Aliasdatensätze auf Yes fest. (Evaluate Target Health wird für einige AWS Ressourcen nicht unterstützt.)

6. Erstellen Sie von unten in dem Baumdiagramm, das Sie in Schritt 1 angelegt haben, die Aliasdatensätze, die den Datenverkehr zu den Datensätzen weiterleiten, die Sie in Schritt 4 und 5 erstellt haben. Wenn Route 53 einen anderen Zweig der Struktur verwenden soll, wenn alle Nicht-Aliasdatensätze in einem Zweig der Struktur fehlerhaft sind, legen Sie den Wert von Evaluate Target Health für alle Aliasdatensätze auf Yes fest.

   Denken Sie daran, dass Sie keinen Aliasdatensatz erstellen können, der Datenverkehr zu einem anderen Datensatz weiterleitet, bevor Sie den anderen Datensatz erstellt haben.

So funktionieren Zustandsprüfungen in einfachen Amazon Route 53-Konfigurationen

Wenn es zwei oder mehr Ressourcen gibt, die dieselbe Funktion ausführen, beispielsweise zwei oder mehr Webserver für example.com, können Sie die folgenden Zustandsprüfungsfunktionen verwenden, um den Datenverkehr nur zu den fehlerfreien Ressourcen zu leiten:

Überprüfen Sie den Zustand von EC2 Instanzen und anderen Ressourcen (Nicht-Alias-Datensätze)

Wenn Sie Traffic an Ressourcen weiterleiten, für die Sie keine Alias-Datensätze erstellen können, wie z. B. EC2 Instanzen, erstellen Sie einen Datensatz und eine Zustandsprüfung für jede Ressource. Ordnen Sie anschließend jeder Zustandsprüfung den entsprechenden Datensatz zu. Zustandsprüfungen überprüfen regelmäßig den Zustand der entsprechenden Ressourcen, und Route 53 leitet Datenverkehr nur zu den Ressourcen weiter, die von den Zustandsprüfungen als fehlerfrei gemeldet werden.

Evaluieren Sie den Zustand einer AWS Ressource (Alias-Datensätze)

Wenn Sie Aliaseinträge verwenden, um den Verkehr an ausgewählte AWS Ressourcen weiterzuleiten, z. B. an ELB-Load Balancer, können Sie Route 53 so konfigurieren, dass der Zustand der Ressource bewertet wird und der Verkehr nur an fehlerfreie Ressourcen weitergeleitet wird. Wenn Sie einen Aliasdatensatz konfigurieren, um den Zustand einer Ressource zu bewerten, brauchen Sie keine Zustandsprüfung für die Ressource zu erstellen.

Hier ist eine Übersicht, wie Route 53 in einfachen Konfigurationen zum Überprüfen des Zustands der Ressourcen konfiguriert wird:

1. Ermitteln Sie die Ressourcen, die Route 53 überwachen soll. Sie können beispielsweise alle HTTP-Server überwachen, die auf Abfragen für example.com antworten.
2. Sie erstellen Integritätsprüfungen für die Ressourcen, für die Sie keine Aliaseinträge erstellen können, z. B. für EC2 Instanzen oder Server in Ihrem eigenen Rechenzentrum. Geben Sie an, wie Zustandsprüfungsanfragen an die Ressource gesendet werden sollen: welches Protokoll gesendet werden soll (HTTP, HTTPS oder TCP), welche IP-Adresse und welcher Port verwendet werden sollen und bei HTTP/HTTPS-Zustandsprüfungen einen Domänennamen und Pfad.

> **Note**
>
> Wenn Sie Ressourcen verwenden, für die Sie keine Aliasdatensätze erstellen können, z. B. ELB-Load Balancers, erstellen Sie keine Zustandsprüfungen für diese Ressourcen.

In einer häufig verwendeten Konfiguration wird eine Zustandsprüfung für jede Ressource erstellt und die gleich IP-Adresse für die Zustandsprüfung des Endpunkts und der Ressource verwendet. Die Zustandsprüfung sendet Anfragen an die angegebene IP-Adresse.

> **Note**
>
> Route 53 kann den Zustand von Ressourcen, deren IP-Adresse im lokalen, privaten, nicht-routingfähigen oder Multicast-Bereich liegt, nicht überprüfen. Weitere Informationen zu IP-Adressen, für die Sie keine Integritätsprüfungen erstellen können, finden Sie unter RFC 5735, Special Use IPv4 Addresses und RFC 6598, IPv4 IANA-reserviertes Präfix für gemeinsamen Adressraum.

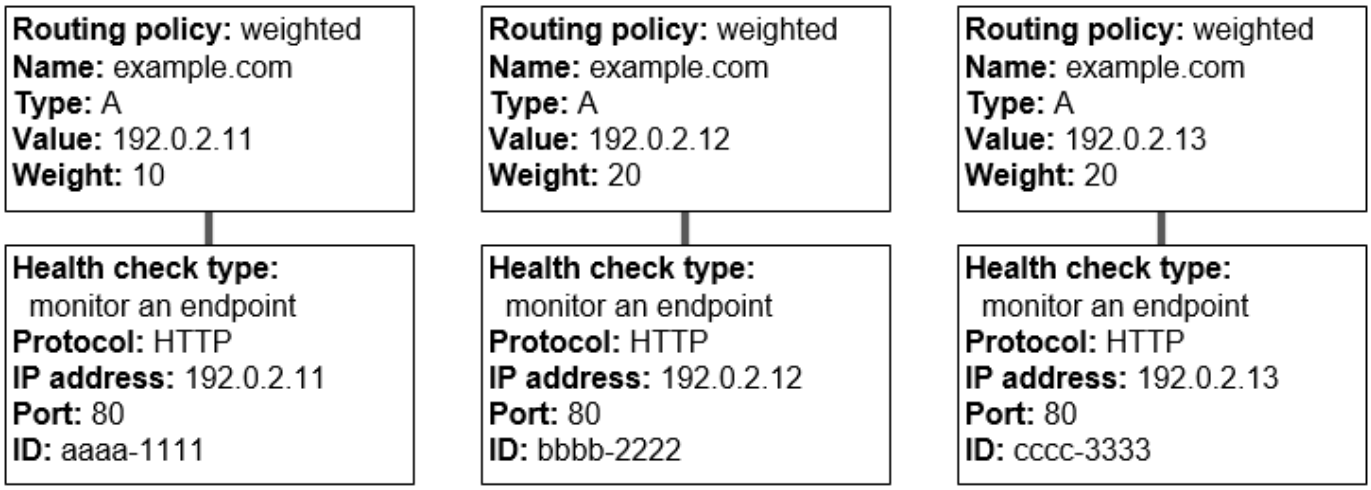
Weitere Informationen zum Erstellen von Zustandsprüfungen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

3. Möglicherweise müssen Sie Router- und Firewall-Regeln so konfigurieren, dass Route 53 regelmäßige Abfragen an die Endpunkte senden kann, die Sie in Ihren Zustandsprüfungen angegeben haben. Weitere Informationen finden Sie unter Konfigurieren von Router- und Firewall-Regeln für Amazon Route 53-Zustandsprüfungen.
4. Erstellen Sie eine Gruppe von Datensätzen für Ihre Ressourcen, z. B. eine Gruppe von gewichteten Datensätzen. Sie können Alias- und Nicht-Aliasdatensätze mischen, aber sie müssen alle denselben Wert für Name, Typeund Routing Policy haben.

   Wie Sie Route 53 zur Überprüfung des Zustands Ihrer Ressourcen konfigurieren, hängt davon ab, ob Sie Alias- oder Nicht-Aliasdatensätze erstellen:

   - Aliasdatensätze - Geben Sie Yes für Evaluate Target Health an.
   - Nicht-Aliasdatensätze - Ordnen Sie die Zustandsprüfungen, die Sie in Schritt 2 erstellt haben, den entsprechenden Datensätzen zu.

Wenn Sie fertig sind, sieht Ihre Konfiguration ähnlich wie das folgende Diagramm aus, das ausschließlich Nicht-Aliasdatensätze enthält.



Weitere Informationen zur Erstellung von Datensätzen mit der Route 53-Konsole finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

5. Wenn Sie Zustandsprüfungen erstellt haben, sendet Route 53 für jede Zustandsprüfung in regelmäßigen Abständen Abfragen an den Endpunkt. Beim Eingang einer DNS-Abfrage wird jedoch keine Zustandsprüfung ausgeführt. Auf der Grundlage der Antworten entscheidet Route 53, ob die Endpunkte fehlerfrei sind, und verwendet diese Informationen, um zu bestimmen, wie auf Abfragen reagiert wird. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

   Route 53 führt keine Zustandsprüfung für die im Datensatz angegebene Ressource aus, z. B. die IP-Adresse in einem A-Datensatz für example.com. Wenn Sie eine Zustandsprüfung mit einem Datensatz verknüpfen, überprüft Route 53 den Zustand des Endpunkts, den Sie in der Zustandsprüfung angegeben haben. Sie können Route 53 auch so konfigurieren, dass der Zustand anderer Integritätsprüfungen oder die Datenströme auf Alarme überwacht werden. CloudWatch Weitere Informationen finden Sie unter Arten von Amazon Route 53-Zustandsprüfungen.

Wenn Route 53 eine Abfrage für example.com erhält, geschieht Folgendes:

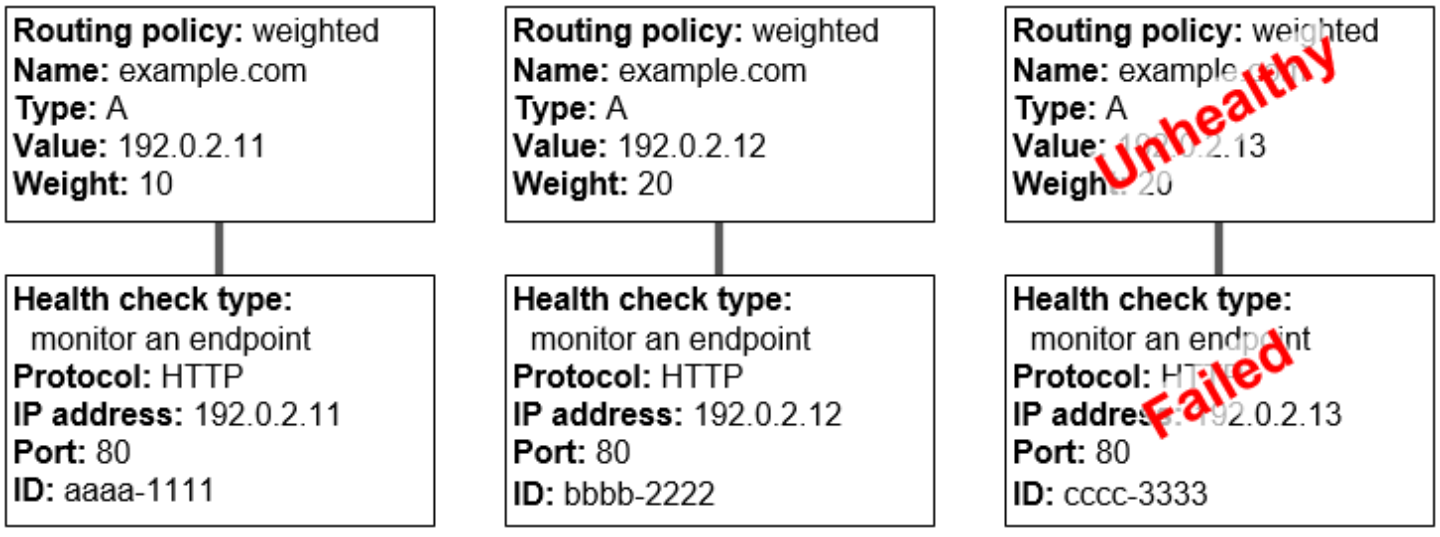
1. Route 53 wählt einen Datensatz basierend auf der Weiterleitungsrichtlinie aus. In diesem Fall wird ein Datensatz basierend auf der Gewichtung ausgewählt.

2. Der aktuelle Zustand des ausgewählten Datensatzes wird durch die Überprüfung des Status der Zustandsprüfung für den jeweiligen Ressourcendatensatz festgestellt.
3. Wenn der ausgewählte Datensatz fehlerhaft ist, wählt Route 53 einen anderen Datensatz aus. Dieses Mal wird der fehlerhafte Datensatz nicht berücksichtigt.

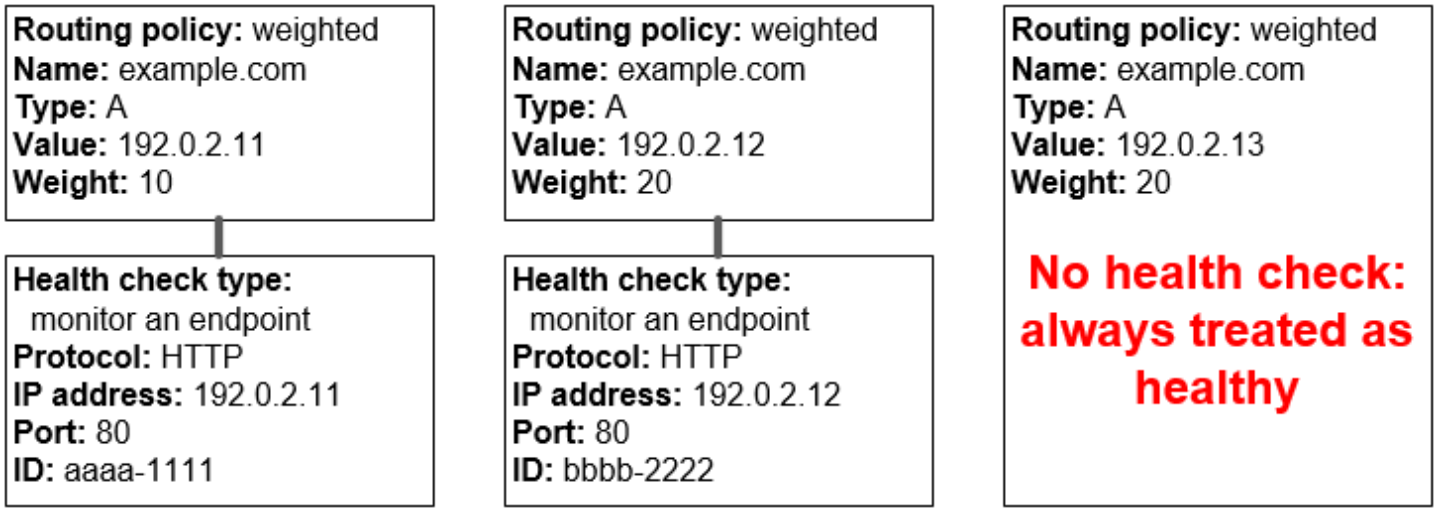
   Weitere Informationen finden Sie unter So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind.
4. Wenn Route 53 einen fehlerfreien Datensatz findet, antwortet es auf die Abfrage mit dem entsprechenden Wert, z. B. der IP-Adresse in einem A-Datensatz.

Das folgende Beispiel zeigt eine Gruppe von gewichteten Datensätzen, in der der dritte Datensatz fehlerhaft ist. Anfänglich wählt Route 53 einen Datensatz basierend auf der Gewichtung aller drei Datensätze aus. Wenn beim ersten Mal der fehlerhafte Datensatz ausgewählt wird, wählt Route 53 einen anderen Datensatz aus. Dieses Mal wird die Gewichtung des dritten Datensatzes in der Berechnung jedoch nicht berücksichtigt:

- Wenn Route 53 beim ersten Mal aus allen drei Datensätzen auswählt, wird in 20 % der Zeit auf Abfragen mit dem ersten Datensatz geantwortet, 10/(10+20+20).
- Wenn Route 53 feststellt, dass der dritte Datensatz fehlerhaft ist, wird in 33 % der Zeit auf Abfragen mit dem ersten Datensatz geantwortet, 10/(10+20).



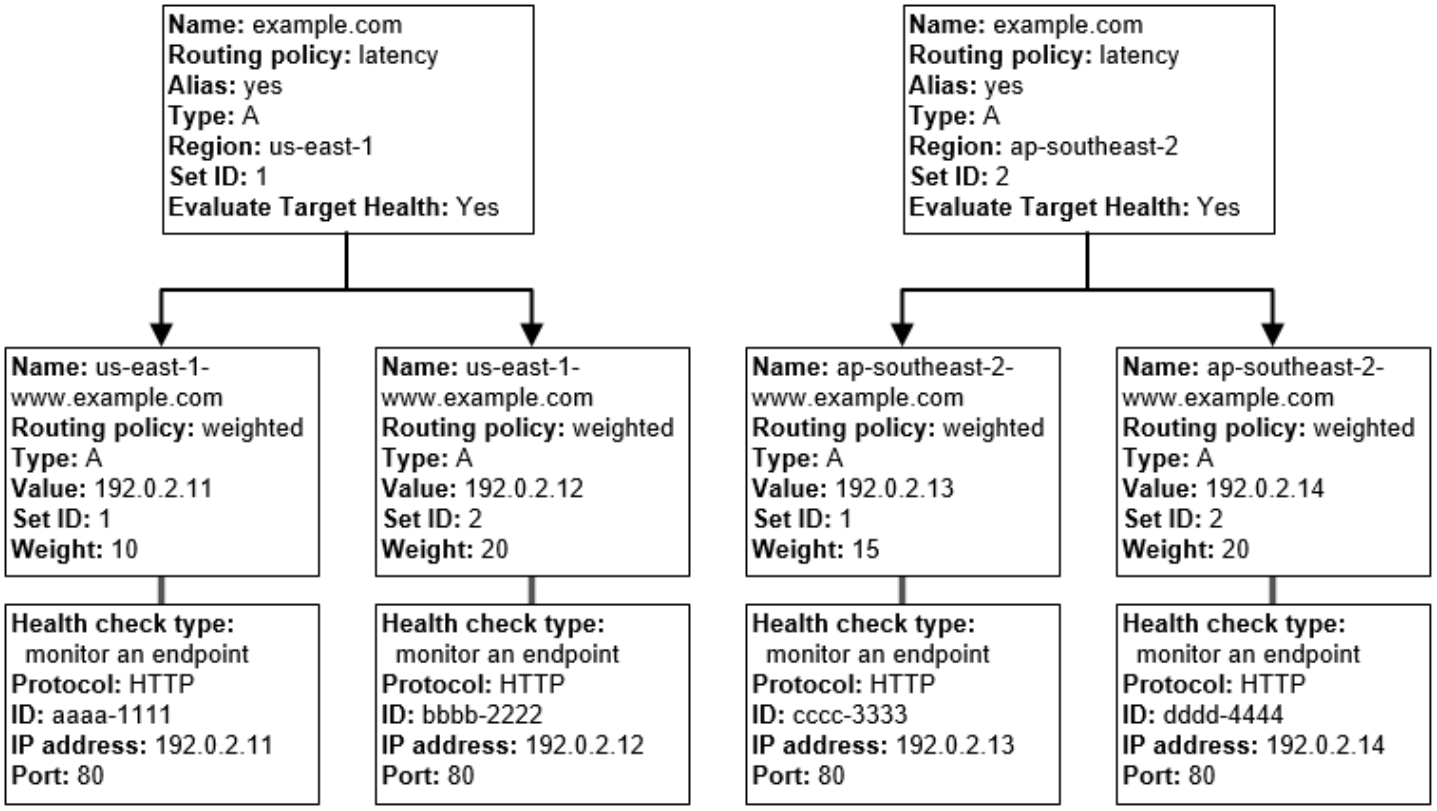
Wenn Sie eine Zustandsprüfung von einem oder mehreren Datensätzen in einer Gruppe von Datensätzen auslassen, hat Route 53 keine Möglichkeit, den Zustand der entsprechenden Ressource zu ermitteln. Route 53 bewertet diese Datensätze als fehlerfrei.



So funktionieren Zustandsprüfungen in komplexen Amazon-Route-53-Konfigurationen

Die Prüfung des Zustands von Ressourcen in komplexen Konfigurationen funktioniert ähnlich wie bei einfachen Konfigurationen. In komplexen Konfigurationen verwenden Sie jedoch eine Kombination aus Aliasdatensätzen (z. B. gewichtete Alias- und Failover-Aliasdatensätze) und Nicht-Aliasdatensätzen, um einen Entscheidungsbaum zu erstellen, mit dem Sie mehr Kontrolle darüber erhalten, wie Route 53 auf Anforderungen reagiert.

Sie können beispielsweise Latenz-Aliasdatensätze verwenden, um eine Region in der Nähe des Benutzers auszuwählen, und gewichtete Datensätze für zwei oder mehr Ressourcen in jeder Region verwenden, um Schutz vor dem Ausfall eines einzelnen Endpunkts oder einer Availability Zone zu bieten. In der folgenden Abbildung ist diese Konfiguration dargestellt.



So werden Amazon EC2 und Route 53 konfiguriert. Beginnen wir am unteren Ende des Baums, da dies die Reihenfolge ist, in der Sie Datensätze erstellen:

- Sie haben zwei EC2 Instances in jeder der beiden Regionen, us-east-1 und ap-southeast-2. Sie möchten, dass Route 53 den Traffic an Ihre EC2 Instances weiterleitet, je nachdem, ob sie fehlerfrei sind. Deshalb erstellen Sie für jede Instance eine Integritätsprüfung. Sie konfigurieren die Zustandsprüfungen so, dass Zustandsprüfungsanfragen an die entsprechende Instance unter der Elastic IP-Adresse für die Instance gesendet werden.

  Route 53 ist ein globaler Service, daher brauchen Sie nicht die Region anzugeben, in der Sie die Zustandsprüfungen erstellen wollen.

- Sie möchten Datenverkehr zu den beiden Instances in jeder Region basierend auf dem Instance-Typ weiterleiten, daher erstellen Sie einen gewichteten Datensatz für jede Instance und geben jedem Datensatz eine Gewichtung. (Sie können die Gewichtung zu einem späteren Zeitpunkt ändern, um mehr oder weniger Datenverkehr zu einer Instance zu leiten.) Sie ordnen jeder Instance auch die entsprechende Zustandsprüfung zu.

  Beim Erstellen der Datensätze verwenden Sie Namen wie us-east-1-www.example.com. und ap-southeast-2-www.example.com. Sie warten, bis Sie zur Spitze des Baums gelangen, bevor Sie

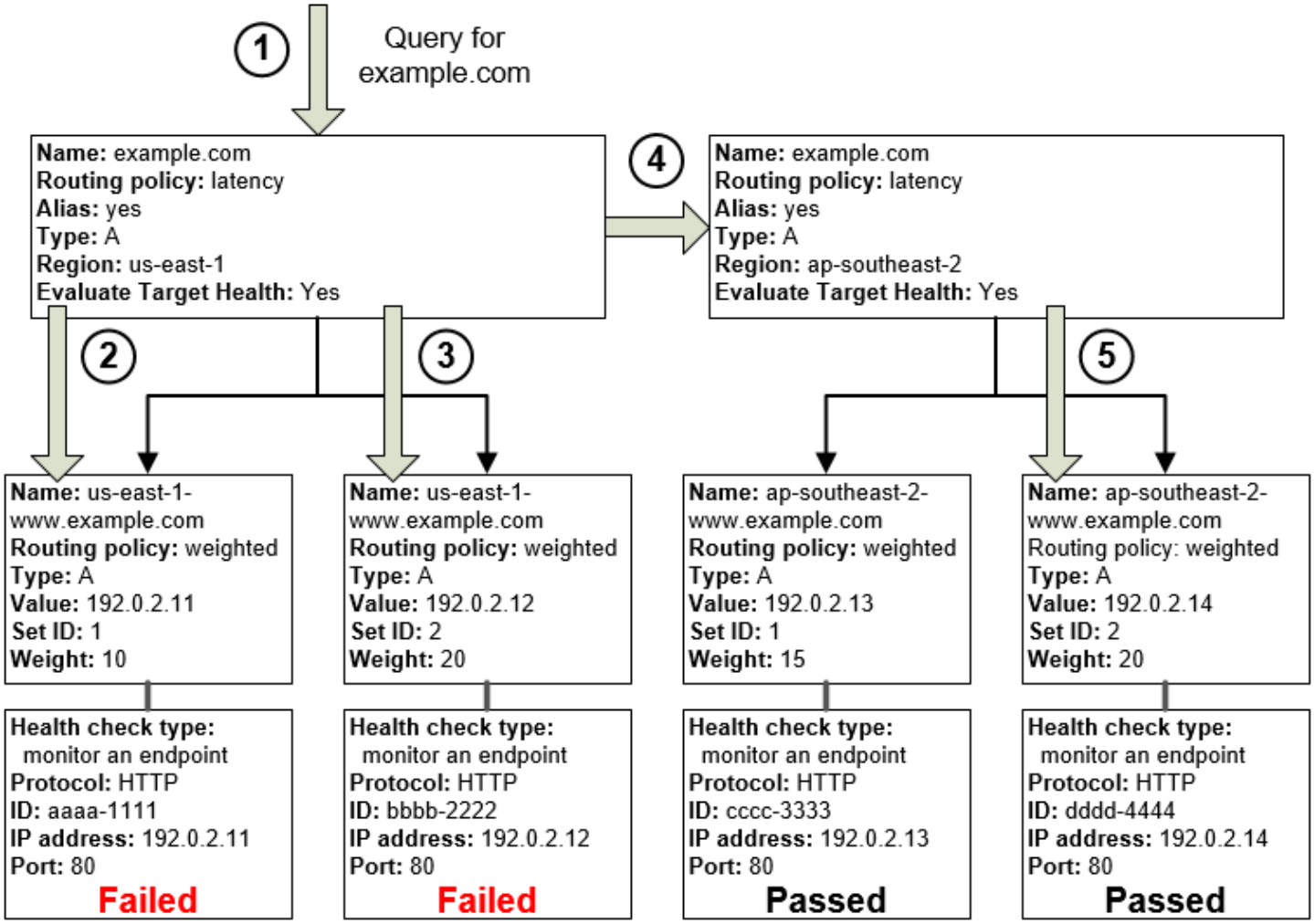
Datensätzen die Namen geben, die Ihre Benutzer verwenden werden, um auf Ihre Website oder Webanwendung zuzugreifen, z. B. example.com.

- Sie möchten Datenverkehr zu der Region mit der niedrigsten Latenz für Ihre Benutzer weiterleiten, daher wählen Sie die Latenz-Routing-Richtlinie für die Datensätze oben im Baum.

  Sie möchten Datenverkehr zu den Datensätzen in den einzelnen Regionen weiterleiten, nicht direkt zu den Ressourcen in jeder Region (die gewichteten Datensätze tun das bereits). Infolgedessen erstellen Sie Latenz-Aliasdatensätze.

  Beim Erstellen von Aliasdatensätzen geben Sie ihnen den Namen, den Ihre Benutzer verwenden sollen, um auf Ihre Website oder Webanwendung zuzugreifen, z. B. example.com. Die Aliasdatensätze leiten den Datenverkehr für example.com zu den Datensätzen us-east-1-www.example.com und ap-southeast-2-www.example.com weiter.

  Für beide Latenz-Aliasdatensätze legen Sie den Wert für Evaluate Target Health auf Yes fest. Dies bewirkt, dass Route 53 prüft, ob es fehlerfreie Ressourcen in einer Region gibt, bevor versucht wird, Datenverkehr dorthin zu leiten. Falls nicht, wählt Route 53 eine fehlerfreie Ressource in der anderen Region aus.



Das vorherige Diagramm veranschaulicht die folgende Ereignissequenz:

1. Route 53 erhält eine Abfrage für example.com. Basierend auf der Latenz für den Benutzer, der die Abfrage sendet, wählt Route 53 den Latenz-Aliasdatensatz für die Region us-east-1 aus.
2. Route 53 wählt einen gewichteten Datensatz basierend auf der Gewichtung aus. Evaluate Target Health ist für den Latenz-Aliasdatensatz auf Yes festgelegt, sodass Route 53 den Zustand des ausgewählten gewichteten Datensatzes prüft.
3. Die Zustandsprüfung ist fehlgeschlagen, sodass Route 53 einen anderen gewichteten Datensatz basierend auf der Gewichtung auswählt und dessen Zustand prüft. Der Datensatz ist ebenfalls fehlerhaft.
4. Route 53 verlässt diesen Zweig, sucht nach dem Latenz-Aliasdatensatz mit der nächstbesten Latenz und wählt den Datensatz für ap-southeast-2 aus.

5. Route 53 wählt erneut einen Datensatz basierend auf der Gewichtung aus und prüft den Zustand der ausgewählten Ressource. Die Ressource ist fehlerfrei, daher gibt Route 53 den entsprechenden Wert als Reaktion auf die Abfrage zurück.

Themen

Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?

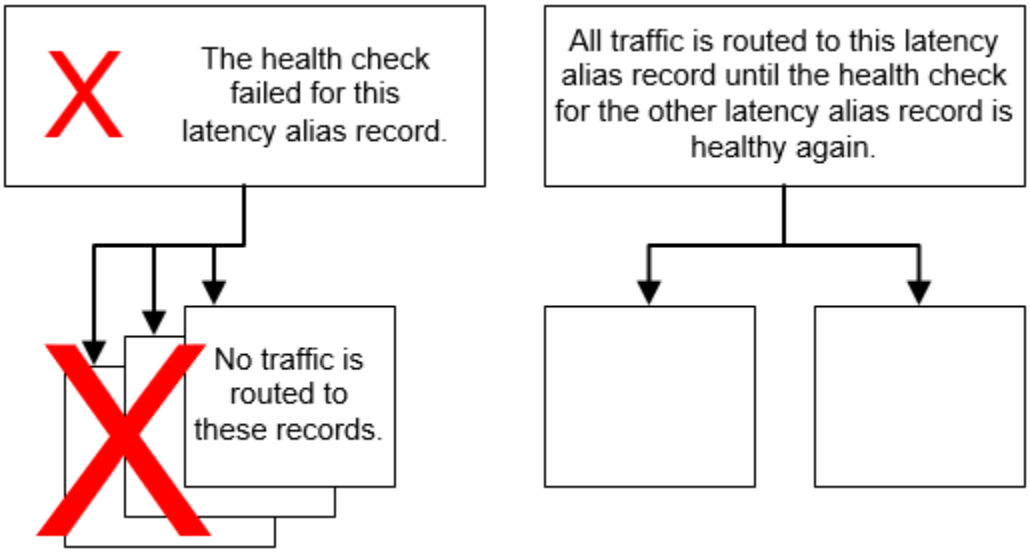
Sie können eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und/oder den Wert für Evaluate Target Health auf Yes festlegen. Es ist in der Regel jedoch nützlicher, wenn Route 53 Abfragen basierend auf dem Zustand der zugrundeliegenden Ressourcen beantwortet. d. h. der HTTP-Server, der Datenbankserver und anderer Ressourcen, auf die sich die Aliasdatensätze beziehen. Angenommen, Sie haben folgende Konfiguration:

- Sie ordnen einem Latenz-Aliasdatensatz, für den das Aliasziel eine Gruppe von gewichteten Datensätzen ist, eine Zustandsprüfung zu.
- Sie legen für den Latenz-Aliasdatensatz den Wert von Evaluate Target Health auf Yes fest.

In dieser Konfiguration müssen die beiden folgenden Bedingungen erfüllt sein, bevor Route 53 den entsprechenden Wert für einen gewichteten Datensatz zurückgibt:

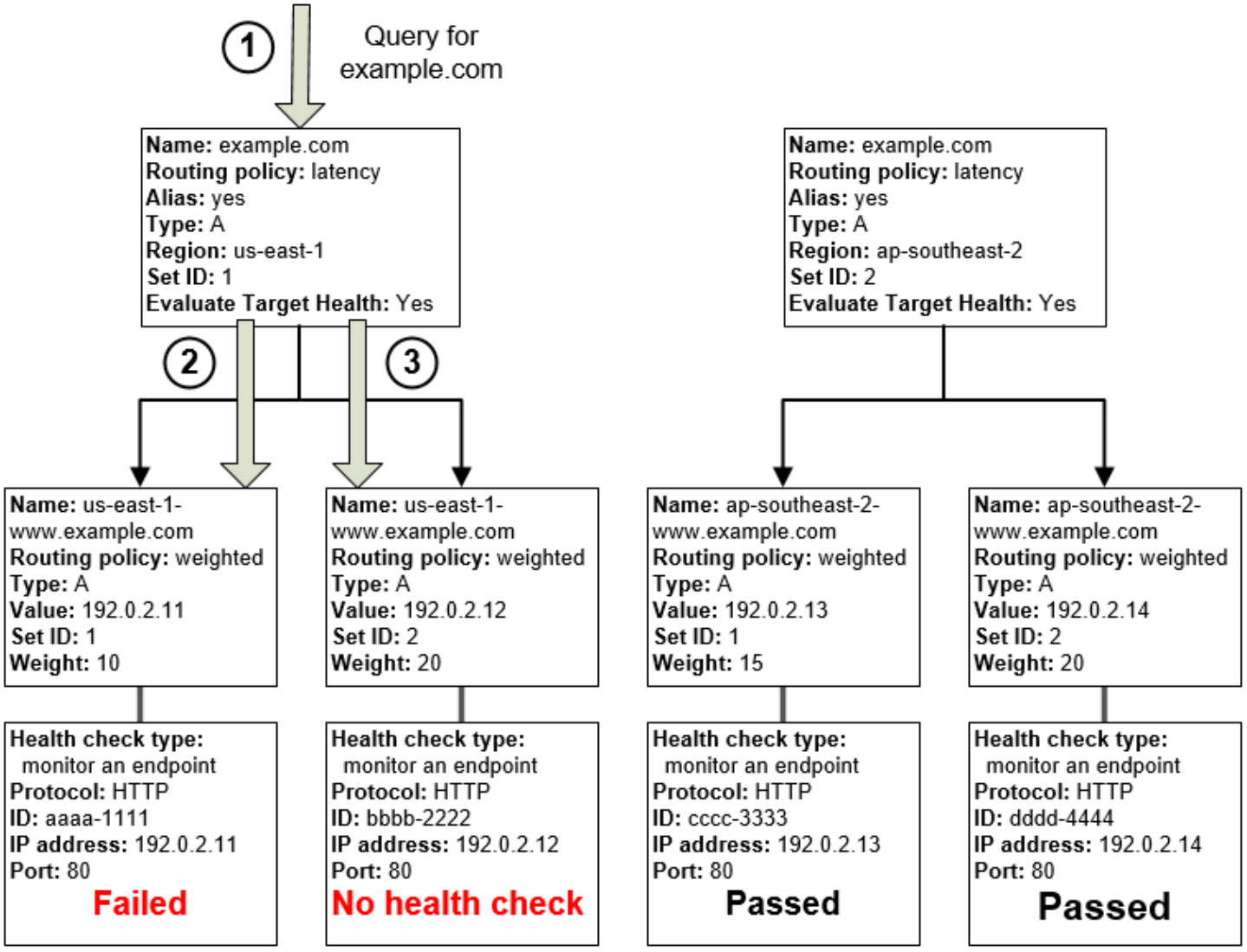
- Die dem Latenz-Aliasdatensatz zugeordnete Zustandsprüfung muss erfolgreich sein.
- Mindestens ein gewichteter Ressourcendatensatz muss als fehlerfrei bewertet werden, weil er entweder einer bestandenen Zustandsprüfung zugeordnet ist oder weil er keiner Zustandsprüfung zugeordnet ist. Im zweiten Fall bewertet Route 53 den gewichteten Datensatz als fehlerfrei.

In der folgenden Abbildung ist die Zustandsprüfung für den Latenz-Aliasdatensatz oben links fehlgeschlagen. Infolgedessen hört Route 53 auf, Abfragen mithilfe eines der gewichteten Datensätze zu beantworten, auf die sich der Latenz-Aliasdatensatz bezieht, auch wenn diese alle fehlerfrei sind. Route 53 berücksichtigt diese gewichteten Datensätze erst dann wieder, wenn die Zustandsprüfung für den Latenz-Aliasdatensatz wieder fehlerfrei ist. (Ausnahmen sind unter So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind beschrieben.)



Was geschieht, wenn Sie Zustandsprüfungen überspringen?

In einer komplexen Konfiguration ist es wichtig, allen Nicht-Aliasdatensätzen Zustandsprüfungen zuzuordnen. Im folgenden Beispiel fehlt eine Zustandsprüfung für einen der gewichteten Datensätze in der Region us-east-1.



Wenn Sie eine Zustandsprüfung für einen Nicht-Aliasdatensatz in dieser Konfiguration überspringen, geschieht Folgendes:

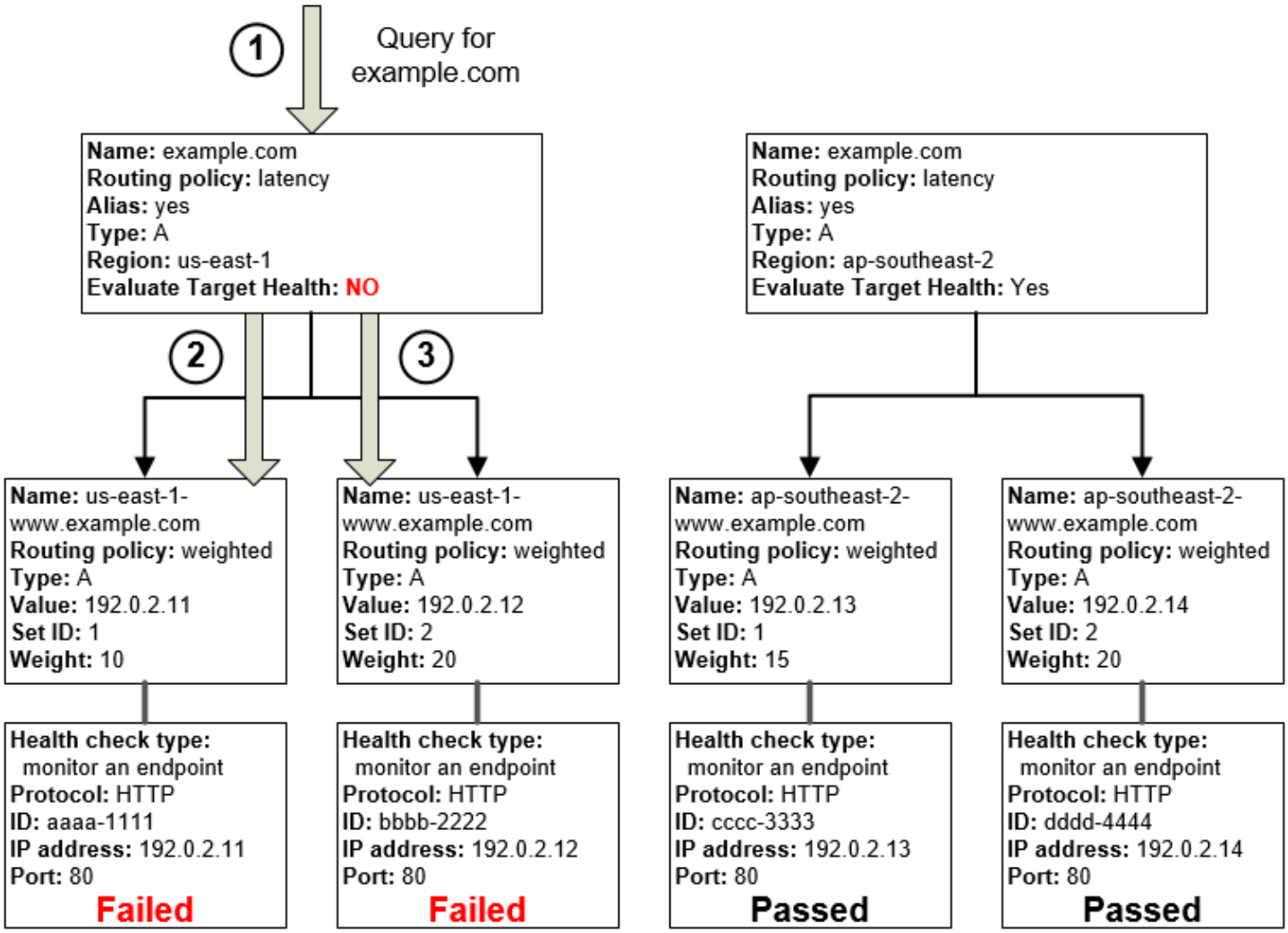
1. Route 53 erhält eine Abfrage für example.com. Basierend auf der Latenz für den Benutzer, der die Abfrage sendet, wählt Route 53 den Latenz-Aliasdatensatz für die Region us-east-1 aus.
2. Route 53 sucht das Aliasziel für den Latenz-Aliasdatensatz und prüft den Status der entsprechenden Zustandsprüfungen. Die Zustandsprüfung für einen gewichteten Datensatz ist fehlgeschlagen, sodass der Datensatz nicht berücksichtigt wird.
3. Der andere gewichtete Datensatz im Aliasziel für die Region us-east-1 besitzt keine Zustandsprüfung. Die entsprechenden Ressourcen könnten fehlerfrei oder fehlerhaft sein, aber ohne eine Zustandsprüfung kann Route 53 dies nicht erkennen. Route 53 geht davon aus, dass

die Ressource fehlerfrei ist, und gibt den entsprechenden Wert als Reaktion auf die Abfrage zurück.

Was geschieht, wenn Sie "Evaluate Target Health" auf "No" setzen?

Im Allgemeinen sollten Sie Evaluate Target Health für alle Aliasdatensätze in einer Struktur auf Yes festlegen. Wenn Sie Evaluate Target Health auf No festlegen, leitet Route 53 weiterhin auch dann Datenverkehr zu den Datensätzen, auf die ein Aliasdatensatz verweist, wenn die Zustandsprüfungen für diese Datensätze fehlschlagen.

Im folgenden Beispiel sind allen gewichteten Datensätzen Zustandsprüfungen zugeordnet, Evaluate Target Health ist für den Latenz-Aliasdatensatz für die Region us-east-1 jedoch auf No festgelegt:



Wenn Sie Evaluate Target Health für einen Aliasdatensatz in dieser Konfiguration auf No festlegen, geschieht Folgendes:

1. Route 53 erhält eine Abfrage für example.com. Basierend auf der Latenz für den Benutzer, der die Abfrage sendet, wählt Route 53 den Latenz-Aliasdatensatz für die Region us-east-1 aus.
2. Route 53 bestimmt, welches Aliasziel für den Latenz-Aliasdatensatz verwendet wird, und prüft den Status der entsprechenden Zustandsprüfungen. Beide schlagen fehl.
3. Da der Wert von Evaluate Target Health für den Latenz-Aliasdatensatz für die Region us-east-1 auf No festgelegt ist, muss Route 53 einen Datensatz in diesem Zweig auswählen, statt den Zweig zu verlassen und nach einem fehlerfreien Datensatz in der Region ap-southeast-2 zu suchen.

So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind

Wenn Sie Zustandsprüfungen für alle Datensätze in einer Gruppe von Datensätzen konfigurieren, die denselben Namen, denselben Typ (z. B. A oder AAAA) und dieselbe Routing-Richtlinie (z. B. gewichtet oder Failover) haben, beantwortet Route 53 DNS-Abfragen, indem ein fehlerfreier Datensatz ausgewählt und der entsprechende Wert von diesem Datensatz zurückgegeben wird.

Nehmen wir zum Beispiel an, sie erstellen drei gewichtete A-Datensätze und weisen allen dreien Zustandsprüfungen zu. Wenn die Zustandsprüfung für einen der Datensätze fehlerhaft ist, beantwortet Route 53 DNS-Abfragen mit den IP-Adressen in einem der anderen beiden Datensätze.

So wählt Route 53 einen fehlerfreien Datensatz aus:

1. Route 53 wählt zunächst einen Datensatz basierend auf der Routing-Richtlinie und auf den Werten aus, die Sie für jeden Datensatz angeben. Für gewichtete Datensätze wählt Route 53 beispielsweise einen Datensatz basierend auf der Gewichtung aus, die Sie für die einzelnen Datensätze angegeben haben.
2. Route 53 ermittelt, ob der Datensatz fehlerfrei ist:
   - Nicht-Aliasdatensätze mit zugeordneter Zustandsprüfung - Wenn Sie einem Nicht-Aliasdatensatz eine Zustandsprüfung zugeordnet haben, überprüft Route 53 den aktuellen Status der Zustandsprüfung.

     Route 53 überprüft regelmäßig den Zustand des Endpunkts, der in einer Zustandsprüfung angegeben ist. Bei Eingang einer DNS-Abfrage wird keine Zustandsprüfung durchgeführt.

Sie können Aliasdatensätzen Zustandsprüfungen zuordnen, aber wir empfehlen, dies nur bei Nicht-Aliasdatensätzen zu tun. Weitere Informationen finden Sie unter Was geschieht, wenn Sie eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen?.

- Aliasdatensatz, bei dem "Evaluate Target Health" auf "Yes" gesetzt ist Route 53 überprüft den Zustand der Ressource, auf die der Aliasdatensatz verweist, z. B. einen ELB-Load Balancer oder einen anderen Datensatz in derselben gehosteten Zone.

3. Wenn der Datensatz fehlerfrei ist, antwortet Route 53 auf die Abfrage mit dem entsprechenden Wert, z. B. einer IP-Adresse.

   Wenn der Datensatz fehlerhaft ist, wählt Route 53 anhand derselben Kriterien einen anderen Datensatz aus und wiederholt den Prozess, bis ein fehlerfreier Datensatz gefunden wird.

Route 53 wendet bei der Auswahl eines Datensatzes die folgenden Kriterien an:

Datensätze ohne Zustandsprüfung sind immer fehlerfrei

Wenn einem Datensatz in einer Gruppe von Datensätzen, die denselben Namen und Typ haben, keine Zustandsprüfung zugeordnet ist, bewertet Route 53 sie stets als fehlerfrei und fügt sie stets in mögliche Antworten auf eine Abfrage ein.

Wenn kein Datensatz fehlerfrei ist, werden alle Datensätze als fehlerfrei bewertet

Wenn keiner der Datensätze in einer Gruppe von Datensätzen fehlerfrei ist, muss Route 53 etwas als Antwort auf die DNS-Abfragen zurückgeben, hat jedoch keine Grundlage für die Auswahl eines bestimmten Datensatzes anstelle eines anderen. In diesem Fall bewertet Route 53 alle Datensätze in der Gruppe als fehlerfrei und wählt einen Datensatz auf der Grundlage der Routing-Richtlinie und der Werte aus, die Sie für die einzelnen Datensätze angegeben haben.

Gewichtete Datensätze, die die Gewichtung 0 haben

Wenn Sie Zustandsprüfungen für alle Datensätze in einer Gruppe von gewichteten Datensätzen hinzufügen, Sie einigen Datensätze jedoch Gewichtungen ungleich Null und anderen Gewichtungen gleich Null geben, funktionieren Zustandsprüfungen ebenso, als ob alle Datensätze Gewichtungen ungleich Null hätten, mit den folgenden Ausnahmen:

- Route 53 berücksichtigt zu Beginn nur die mit nicht-null gewichteten Datensätze, wenn vorhanden.
- Wenn alle Datensätze mit einer Gewichtung größer als 0 fehlerhaft sind, berücksichtigt Route 53 die mit Null gewichteten Datensätze.

Da Route 53 unter bestimmten Umständen die mit Null gewichteten Datensätze berücksichtigt, muss sichergestellt werden, dass das mit Null gewichtete Ziel auch eine geeignete Antwort auf eine DNS-Abfrage hat.

Weitere Informationen zu gewichteten Datensätzen finden Sie unter Zustandsprüfungen und gewichtetes Routing.

Alias-Datensätze

Sie können Zustandsprüfungen für Aliasdatensätze auch konfigurieren, indem Sie Evaluate Target Health bei jedem Aliasdatensatz auf Yes setzen. Dies bewirkt, dass Route 53 den Zustand der Ressource bewertet, zu der der Datensatz Datenverkehr leitet, z. B. einem ELB-Load Balancer oder einem anderen Datensatz in derselben gehosteten Zone.

Angenommen, das Aliasziel für einen Aliasdatensatz ist eine Gruppe von gewichteten Datensätzen mit einer Gewichtung, die ungleich Null ist:

- Solange mindestens einer der gewichteten Datensätze fehlerfrei ist, bewertet Route 53 den Aliasdatensatz als fehlerfrei.
- Wenn keiner der gewichteten Datensätze fehlerfrei ist, bewertet Route 53 den Aliasdatensatz als fehlerhaft.
- Route 53 hält die Bewertung von Datensätzen in diesem Zweig an, bis mindestens ein gewichteter Datensatz wieder fehlerfrei ist.

Weitere Informationen finden Sie unter So funktionieren Zustandsprüfungen in komplexen Amazon-Route-53-Konfigurationen.

Failover-Datensätze

Failover-Datensätze funktionieren im Allgemeinen auf die gleiche Weise wie andere Routing-Typen. Sie erstellen Zustandsprüfungen und ordnen sie Nicht-Aliasdatensätzen zu, und Sie setzen Evaluate Target Health bei Aliasdatensätzen auf Yes. Beachten Sie Folgendes:

- Sowohl die primären als auch die sekundären Datensätze können ein Nicht-Aliasdatensatz oder ein Aliasdatensatz sein.
- Wenn Sie den primären und sekundären Failover-Datensätzen Zustandsprüfungen zuordnen, reagiert Route 53 wie folgt auf Abfragen:
  - Wenn Route 53 den primären Datensatz als fehlerfrei betrachtet (wenn die Zustandsprüfung für einen Endpunkt ergibt, dass dieser fehlerfrei ist), gibt Route 53 nur den primären Datensatz als Antwort auf eine DNS-Abfrage zurück.

  - Wenn Route 53 den primären Datensatz als fehlerhaft und den sekundären Datensatz als fehlerfrei betrachtet, gibt Route 53 stattdessen den sekundären Datensatz zurück.
  - Wenn Route 53 sowohl den primären als auch den sekundären Datensatz als fehlerhaft betrachtet, gibt Route 53 den primären Datensatz zurück.
- Wenn Sie den sekundären Datensatz konfigurieren, ist das Hinzufügen einer Zustandsprüfung optional. Wenn Sie die Zustandsprüfung für den sekundären Datensatz überspringen und die Zustandsprüfung für den primären Datensatz einen fehlerhaften Endpunkt ermittelt, beantwortet Route 53 DNS-Abfragen stets mit dem sekundären Datensatz. Dies gilt auch, wenn der sekundäre Datensatz fehlerhaft ist.

Weitere Informationen finden Sie unter den folgenden Themen:

- Konfigurieren von Aktiv/Passiv-Failover mit einer primären und einer sekundären Ressource
- Konfigurieren von Aktiv/Passiv-Failover mit mehreren primären und sekundären Ressourcen

Aktiv/Aktiv- und Aktiv/Passiv-Failover

Sie können die Zustandsprüfung von Route 53 zum Erstellen von Aktiv/Aktiv- und Aktiv/Passiv-Failover-Konfigurationen verwenden. Sie konfigurieren Aktiv/Aktiv-Failover mithilfe einer anderen -Routing-Richtlinie (oder einer Kombination aus Routing-Richtlinien) als Failover und Aktiv/Passiv-Failover mithilfe der Failover-Routing-Richtlinie.

Themen

- Aktiv/Aktiv-Failover
- Aktiv/Passiv-Failover

Aktiv/Aktiv-Failover

Verwenden Sie diese Failover-Konfiguration, wenn alle Ihre Ressourcen die überwiegende Zeit verfügbar sein sollen. Wenn eine Ressource nicht mehr verfügbar ist, kann Route 53 erkennen, dass sie fehlerhaft ist, und sie beenden, auch wenn Sie auf Abfragen antwortet.

Bei Aktiv/Aktiv-Failover sind alle Datensätze, die denselben Namen, Typ (z. B. A oder AAAA) und dieselbe Routing-Richtlinie haben (z. B. gewichtet oder Latenz) aktiv, wenn sie von Route 53 nicht als fehlerhaft bewertet werden. Route 53 kann mit einem beliebigen fehlerfreien Datensatz auf eine DNS-Abfrage antworten.

Aktiv/Passiv-Failover

Verwenden Sie die Konfiguration Aktiv/Passiv-Failover, wenn eine primäre Ressource oder Gruppe von Ressourcen die überwiegende Zeit zur Verfügung stehen soll und eine sekundäre Ressource oder Gruppe von Ressourcen für den Fall auf Standby ist, dass alle primären Ressourcen unverfügbar werden. Wenn Route 53 auf Abfragen antwortet, werden nur fehlerfreie primäre Ressourcen berücksichtigt. Wenn alle primären Ressourcen fehlerhaft sind, beginnt Route 53, nur die fehlerfreien sekundären Ressourcen in Reaktionen auf DNS-Abfragen einzubeziehen.

Themen

Konfigurieren von Aktiv/Passiv-Failover mit einer primären und einer sekundären Ressource

Um eine Aktiv/Passiv-Failover-Konfiguration mit einem primären Datensatz und einem sekundären Datensatz zu erstellen, erstellen Sie einfach die Datensätze und geben Sie Failover als Routing-Richtlinie an. Wenn die primäre Ressource fehlerfrei ist, beantwortet Route 53 DNS-Abfragen mit dem primären Datensatz. Wenn die primäre Ressource fehlerhaft ist, beantwortet Route 53 DNS-Abfragen mit dem sekundären Datensatz.

Konfigurieren von Aktiv/Passiv-Failover mit mehreren primären und sekundären Ressourcen

Sie können dem primären und dem sekundären Datensatz oder beiden auch mehrere Ressourcen zuordnen. Bei dieser Konfiguration bewertet Route 53 den primären Failover-Datensatz als fehlerfrei, wenn mindestens eine der zugeordneten Ressourcen fehlerfrei ist. Weitere Informationen finden Sie unter So wählt Amazon Route 53 Datensätze, wenn Zustandsprüfungen konfiguriert sind.

Führen Sie die folgenden Aufgaben durch, um Aktiv/Passiv-Failover mit mehreren Ressourcen für den primären oder sekundären Datensatz zu konfigurieren.

1. Erstellen Sie eine Integritätsprüfung für jede Ressource, an die Sie den Datenverkehr weiterleiten möchten, z. B. für eine EC2 Instanz oder einen Webserver in Ihrem Rechenzentrum.

   > **Note**
   >
   > Wenn Sie den Datenverkehr an AWS Ressourcen weiterleiten, für die Sie Aliaseinträge erstellen können, erstellen Sie keine Integritätsprüfungen für diese Ressourcen. Setzen

Sie stattdessen beim Erstellen der Aliasdatensätze die Option Evaluate Target Health auf Yes.

Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

2. Erstellen Sie Datensätze für Ihre primären Ressourcen, und geben Sie die folgenden Werte an:
   - Geben Sie allen Datensätzen denselben Namen, Typ und dieselbe Routing-Richtlinie. Sie können beispielsweise drei gewichtete A-Datensätze erstellen, die alle den Namen „failover-primary.example.com“ haben.
   - Wenn Sie AWS Ressourcen verwenden, für die Sie Aliaseinträge erstellen können, geben Sie Ja für Evaluate Target Health an.

     Wenn Sie Ressourcen verwenden, für die Sie keine Aliasdatensätze erstellen können, ordnen Sie jedem Datensatz die entsprechende Zustandsprüfung aus Schritt 1 zu.

   Weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.
3. Falls zutreffend, erstellen Sie Datensätze für Ihre sekundären Ressourcen, und geben Sie die folgenden Werte an:
   - Geben Sie allen Datensätzen denselben Namen, Typ und dieselbe Routing-Richtlinie. Sie können beispielsweise drei gewichtete A-Datensätze erstellen, die alle den Namen „failover-secondary.example.com“ haben.
   - Wenn Sie AWS Ressourcen verwenden, für die Sie Aliaseinträge erstellen können, geben Sie Ja für Evaluate Target Health an.

     Wenn Sie Ressourcen verwenden, für die Sie keine Aliasdatensätze erstellen können, ordnen Sie jedem Datensatz die entsprechende Zustandsprüfung aus Schritt 1 zu.

> **Note**
>
> Einige Kunden verwenden einen Webserver als primäre Ressource und einen als Website-Endpunkt konfigurierten Amazon S3-Bucket als sekundäre Ressource. Der S3-Bucket enthält eine einfache Meldung mit dem Inhalt „vorübergehend nicht verfügbar“. Wenn Sie diese Konfiguration verwenden, überspringen Sie diesen Schritt und erstellen Sie nur einen Failover-Aliasdatensatz für die sekundäre Ressource in Schritt 4.

4. Erstellen Sie zwei Failover-Aliasdatensätze, einen primären und einen sekundären, und geben Sie die folgenden Werte an:

   Primärer Datensatz

   - Name - Geben Sie den Namen der Domäne (example.com) oder Unterdomäne (www.example.com) an, zu der Route 53 Datenverkehr leiten soll.
   - Alias - Geben Sie Yes an.
   - Alias-Ziel - Geben Sie den Namen der Datensätze an, die Sie in Schritt 2 erstellt haben.
   - Routing-Richtlinie - Geben Sie Failover an.
   - Failover-Datensatztyp - Geben Sie Primary an.
   - Zustand des Ziels bewerten - Geben Sie Yes an.
   - Zustandsprüfung zuordnen - Geben Sie No an.

   Sekundärer Datensatz

   - Name - Geben Sie denselben Namen wie für den primären Datensatz an.
   - Alias - Geben Sie Yes an.
   - Alias-Ziel - Wenn Sie Datensätze für Ihre sekundäre Ressource in Schritt 3 erstellt haben, geben Sie den Namen der Datensätze an. Wenn Sie einen Amazon S3-Bucket als sekundäre Ressource verwenden, geben Sie den DNS-Namen des Website-Endpunkts an.
   - Routing-Richtlinie - Geben Sie Failover an.
   - Failover-Datensatztyp - Geben Sie Secondary an.
   - Zustand des Ziels bewerten - Geben Sie Yes an.
   - Zustandsprüfung zuordnen - Geben Sie No an.

Konfigurieren von Aktiv/Passiv-Failover mit gewichteten Datensätzen

Mit Einschränkungen können Sie auch gewichtete Datensätze für Aktiv/Passiv-Failover verwenden. Wenn Sie für einige Datensätze Gewichtungen ungleich Null und für andere Datensätze Gewichtungen gleich Null angeben, beantwortet Route 53 DNS-Abfragen nur mit fehlerfreien Datensätzen, die Gewichtungen ungleich Null haben. Wenn alle Datensätze mit einer Gewichtung größer als 0 fehlerhaft sind, beantwortet Route 53 Abfragen mit gleich Null gewichteten Datensätzen.

> **Note**
>
> Erst wenn alle Datensätze mit Gewichtungen ungleich Null fehlerhaft sind, beantwortet Route 53 DNS-Abfragen mit Datensätzen, die eine Gewichtung von Null haben. Dies kann

Ihre Webanwendung oder Website unzuverlässig machen, wenn die letzte fehlerfreie Ressource, z. B. ein Webserver, den Datenverkehr nicht verarbeiten kann, wenn andere Ressourcen nicht verfügbar sind.

Konfigurieren von Failover in einer privaten gehosteten Zone

Wenn Sie Failover-Datensätze in einer privaten gehosteten Zone erstellen, beachten Sie die folgenden Hinweise:

- Route 53-Zustandsprüfungen befinden sich außerhalb der VPC. Um den Zustand eines IP-Adresse-Endpunkts in einer VPC über die IP-Adresse zu prüfen, müssen Sie der Instance in der VPC eine öffentliche IP-Adresse zuweisen.
- Sie können eine CloudWatch Metrik erstellen, der Metrik einen Alarm zuordnen und dann eine Integritätsprüfung durchführen, die auf dem Datenstrom für den Alarm basiert. Sie können beispielsweise eine CloudWatch Metrik erstellen, die den Status der EC2 `StatusCheckFailed` Metrik überprüft, der Metrik einen Alarm hinzufügen und dann eine Zustandsprüfung erstellen, die auf dem Datenstrom für den Alarm basiert, um Instanzen innerhalb einer Virtual Private Cloud (VPC) zu überprüfen, die nur private IP-Adressen haben. Informationen zum Erstellen von CloudWatch Metriken und Alarmen mithilfe der CloudWatch Konsole finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Weitere Informationen erhalten Sie unter Arbeiten mit privat gehosteten Zonen und Überwachung von Zustandsprüfungen mit CloudWatch.

So vermeidet Amazon Route 53 Failover-Probleme

Die von Amazon Route 53 implementierten Failover-Algorithmen dienen nicht nur dazu, Datenverkehr an funktionsfähige Endpunkte weiterzuleiten, sondern auch eine Eskalation von Notfällen aufgrund falsch konfigurierter Zustandsprüfungen und Anwendungen, überlasteter Endpunkte und ausgefallener Partitionen zu verhindern.

Themen

- So vermeidet Amazon Route 53 kaskadierende Fehler
- So verarbeitet Amazon Route 53 Internetpartitionen

So vermeidet Amazon Route 53 kaskadierende Fehler

Als erste Verteidigung gegen Cascading-Ausfälle verfügt jeder Routingalgorithmus für Anforderungen (z. B. gewichtet und Failover) über einen Modus, der als letztes Mittel aktiviert wird. Wenn in diesem speziellen Modus alle Datensätze als fehlerhaft betrachtet werden, setzt der Route 53-Algorithmus den Zustand aller Datensätze auf fehlerfrei zurück.

Wenn beispielsweise alle Instances einer Anwendung auf mehreren Hosts Anforderungen für Zustandsprüfungen ablehnen, wählen die Route 53-Server trotzdem eine Antwort aus und geben sie zurück, anstatt keine DNS-Antwort oder eine NXDOMAIN-Antwort (nicht vorhandene Domäne) zurückzugeben. Eine Anwendung kann Benutzern zwar antworten, aber die Zustandsprüfungen dennoch nicht bestehen, und bietet damit Schutz gegen eine falsche Konfiguration.

Wenn eine Anwendung überlastet ist und einer von drei Endpunkten bei den Zustandsprüfungen fehlschlägt und von den Route 53-DNS-Antworten ausgeschlossen wird, verteilt Route 53 Antworten zwischen den beiden verbleibenden Endpunkten. Wenn die verbleibenden Endpunkte die zusätzliche Last nicht verarbeiten können und fehlschlagen, verteilt Route 53 die Antworten wieder auf alle drei Endpunkte.

So verarbeitet Amazon Route 53 Internetpartitionen

Obwohl es ungewöhnlich ist, gibt es gelegentlich erhebliche Internetpartitionen. Das bedeutet, dass große geografische Regionen nicht mehr über das Internet miteinander kommunizieren können. Während dieser Partitionen können die Route 53-Standorte unterschiedliche Schlüsse über den Gesundheitszustand eines Endpunkts ziehen und sich von dem Status unterscheiden, an den gemeldet wurde CloudWatch. Route 53-Zustandsprüfer in jeder AWS Region senden ständig Statusmeldungen an alle Route 53-Standorte. Während der Internetpartitionen haben die einzelnen Route 53-Standorte möglicherweise nur Zugriff auf eine Teilmenge dieser Status, in der Regel von den Status ihrer am nächsten gelegenen Regionen.

Während einer Internetpartition, die sich auf die Konnektivität zu und von DNS-Servern in Südamerika auswirkt, können die Route 53-DNS-Server in der Region Südamerika (São Paulo) guten Zugriff auf Endpunkte für Zustandsprüfungen in der AWS -Region , aber schlechten Zugriff auf Endpunkte an anderen Standorten haben. Gleichzeitig kann Route 53 in USA Ost (Ohio) einen unzureichenden Zugriff auf Endpunkte für Zustandsprüfungen in der Region Südamerika (São Paulo) haben und daraus schließen, dass die entsprechenden Datensätze fehlerhaft sind.

Partitionen wie diese können Situationen hervorrufen, in denen Route 53-Standorte basierend auf der lokalen Sichtbarkeit dieser Endpunkte unterschiedliche Schlussfolgerungen über den Zustand von

Endpunkten ziehen. Dies ist der Grund, warum jeder Route 53-Standort einen Endpunkt als fehlerfrei betrachtet, wenn er nur von einem Teil der erreichbaren Zustandsprüfungen als fehlerfrei betrachtet wird.

Benennen und Verwenden von Tags für Zustandsprüfungen

Sie können den Amazon Route 53-Zustandsprüfungen Tags hinzufügen, mit denen Sie jeder Zustandsprüfung einen Namen geben können, der verständlicher als die Zustandsprüfungs-ID ist. Dabei handelt es sich um dieselben Tags, mit denen AWS Fakturierung und Kostenmanagement Sie Ihre Rechnung organisieren können AWS . Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwendung von Kostenzuordnungs-Tags für benutzerdefinierte Fakturierungsberichte im AWS Billing Benutzerhandbuch.

Jeder Tag besteht aus einem Schlüssel (der Name des Tags) und einem Wert, die Sie beide selbst definieren können. Wenn Sie Tags zu einer Zustandsprüfung hinzufügen, empfehlen wir, ein Tag hinzuzufügen, das die folgenden Werte für den Schlüssel und den Wert hat:

- Schlüssel – Name
- Wert - der Name, den Sie der Zustandsprüfung geben wollen

Der Wert des Tags Name erscheint in der Liste der Zustandsprüfungen in der Route 53-Konsole, mit der Sie Zustandsprüfungen auf einfache Weise unterscheiden können. Um andere Tags für eine Zustandsprüfung anzuzeigen, wählen Sie die Zustandsprüfung und anschließend die Registerkarte Tags aus.

Weitere Informationen zu Tags finden Sie in den folgenden Themen:

- Informationen zum Hinzufügen, Bearbeiten oder Löschen des Tags Name beim Hinzufügen und Bearbeiten von Zustandsprüfungen in der Route 53-Konsole finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.
- Eine Übersicht über das Markieren von Route 53-Ressourcen finden Sie unter Amazon-Route-53-Ressourcen-Markierung.

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags pro Ressource — 50 auf der neuen Konsole und 10 auf der alten Konsole.
- Maximale Schlüssellänge – 128 Unicode-Zeichen
- Maximale Wertlänge – 256 Unicode-Zeichen
- Gültige Werte für Key (Schlüssel) und Value (Wert) Groß- und Kleinbuchstaben im UTF-8-Zeichensatz, Zahlen, Leerzeichen und die folgenden Zeichen: _ . : / = + - and @
- Bei Tag-Schlüsseln und -Werten muss die Groß-/Kleinschreibung beachtet werden
- Verwenden Sie das `aws:` Präfix weder für Schlüssel noch für Werte; es ist für die AWS Verwendung reserviert

Hinzufügen, Bearbeiten und Löschen von Tags für Zustandsprüfungen

Das folgende Verfahren veranschaulicht, wie Tags für die Zustandsprüfungen in der Route 53-Konsole verwendet werden.

> **Note**
>
> Wir aktualisieren die Health Checks-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So fügen Sie Tags zu Zustandsprüfungen hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID der Zustandsprüfung aus, für die Sie Tags hinzufügen möchten.
4. Wählen Sie auf der unteren Seite den Tab „Tags“ und dann „Verwalten“ und dann „Neue Tags hinzufügen“ aus.

5. Geben Sie einen Namen für das Tag in das Feld Schlüssel und einen Wert in das Feld Wert ein.
6. Wählen Sie Speichern.

So bearbeiten Sie Tags für Zustandsprüfungen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID einer Zustandsprüfung aus.
4. Wählen Sie im unteren Bereich die Registerkarte „Tags“ und dann „Verwalten“ aus.
5. Sie können jetzt weitere Tags bearbeiten und hinzufügen.
6. Wählen Sie Speichern.

So löschen Sie Tags für Zustandsprüfungen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID einer Zustandsprüfung aus.
4. Wählen Sie im unteren Bereich die Registerkarte „Tags“ und dann „Verwalten“ aus.
5. Wählen Sie neben dem Tag, das Sie löschen möchten, die Option Entfernen aus.
6. Wählen Sie Speichern.

Old console

So fügen Sie Tags zu Zustandsprüfungen hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie eine Zustandsprüfung oder wählen Sie mehrere Zustandsprüfungen, wenn Sie mehreren Zustandsprüfungen den gleichen Tag hinzufügen möchten.

4. Wählen Sie im unteren Bereich die Registerkarte Tags aus und klicken Sie dann auf die Schaltfläche Add/Edit Tags.
5. Geben Sie im Dialogfeld Add/Edit Tags einen Namen für die Tags in das Feld Key ein, und geben Sie einen Wert in das Feld Value ein.
6. Wählen Sie Apply changes.

So bearbeiten Sie Tags für Zustandsprüfungen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie eine Zustandsprüfung aus.

   Wenn Sie mehrere Zustandsprüfungen auswählen, die den gleichen Tag haben, können Sie den Wert nicht für alle Tags gleichzeitig bearbeiten. Beachten Sie jedoch, dass Sie den Wert eines Tags bearbeiten können, der in mehreren Zustandsprüfungen auftritt, wenn Sie Zustandsprüfungen, die den Tag enthalten, und mindestens eine Zustandsprüfung auswählen, die den Tag nicht enthält.

   Beispiel: Sie haben mehrere Zustandsprüfungen mit dem Tag Cost Center sowie eine Zustandsprüfung, die diesen Tag nicht enthält. Sie wählen die Option zum Hinzufügen eines Tags und geben Cost Center für den Schlüssel und 777 für den Wert an. Für die ausgewählten Zustandsprüfungen, die bereits über einen Cost Center-Tag verfügen, ändert Route 53 den Wert in 777. Für die eine Zustandsprüfung, die keinen Cost Center-Tag hat, fügt Route 53 einen Tag hinzu und setzt den Wert auf 777.
4. Wählen Sie im unteren Bereich die Registerkarte Tags aus und klicken Sie dann auf die Schaltfläche Add/Edit Tags.
5. Bearbeiten Sie den Wert im Dialogfeld Add/Edit Tags.
6. Wählen Sie Speichern.

So löschen Sie Tags für Zustandsprüfungen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.

3. Wählen Sie eine Zustandsprüfung oder wählen Sie mehrere Zustandsprüfungen, wenn Sie in mehreren Zustandsprüfungen den gleichen Tag löschen möchten.
4. Wählen Sie im unteren Bereich die Registerkarte Tags aus und klicken Sie dann auf die Schaltfläche Add/Edit Tags.
5. Wählen Sie im Dialogfeld „Tags hinzufügen/bearbeiten“ das *X* neben dem Tag aus, das Sie löschen möchten.
6. Wählen Sie Speichern.

Verwendung von Zustandsprüfungen mit Amazon Route 53-API-Versionen vor 2012-12-12

Zustandsprüfungen werden ab Version 2012-12-12 der Amazon Route 53-API unterstützt. Wenn eine gehostete Zone Datensätze enthält, für die Zustandsprüfungen konfiguriert sind, wird die ausschließliche Verwendung der API 2012-12-12 oder höher empfohlen. Bitte beachten Sie die folgenden Einschränkungen zur Verwendung von Zustandsprüfungen mit früheren API-Versionen.

- Die Aktion `ChangeResourceRecordSets` kann keine Datensätze erstellen oder löschen, die die Elemente `EvaluateTargetHealth`, `Failover` oder `HealthCheckId` enthalten.
- Die Aktion `ListResourceRecordSets` kann Datensätze auflisten, die diese Elemente enthalten. Diese Elemente sind jedoch nicht in der Ausgabe enthalten. Das Element `Value` der Antwort enthält die Meldung, dass der Datensatz ein nicht unterstütztes Attribut enthält.

Den Status von Zustandsprüfungen überwachen und Benachrichtigungen erhalten

Sie überwachen den Status Ihrer Zustandsprüfungen in der Amazon Route 53-Konsole. Sie können auch CloudWatch Alarme einrichten und automatische Benachrichtigungen erhalten, wenn sich der Status Ihres Gesundheitschecks ändert.

Themen

Anzeigen von Zustandsprüfungsstatus und dem Grund für Zustandsprüfungsausfälle

Auf der Route 53-Konsole können Sie den Status (fehlerfrei oder fehlerhaft) Ihrer Zustandsprüfungen laut Berichten der -Zustandsprüfer einsehen. Für alle Zustandsprüfungen mit Ausnahme von berechneten Zustandsprüfungen können Sie auch den Grund für den letzten Ausfall der Zustandsprüfung einsehen, z. B. Zustandsprüfer konnten keine Verbindung mit dem Endpunkt herstellen.

> **Note**
>
> Wir aktualisieren die Konsole für Gesundheitschecks für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Um den Status und den Grund des letzten Fehlers für eine Zustandsprüfung anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Eine Übersicht über den Status Ihrer Zustandsprüfungen – fehlerfrei oder fehlerhaft – finden Sie in der Spalte Status. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.
4. Für alle Zustandsprüfungen mit Ausnahme von berechneten Zustandsprüfungen können Sie den Status der Route 53-Zustandsprüfer, die den Status eines angegebenen Endpunkts überprüfen, anzeigen.
5. Wählen Sie die verknüpfte ID der Zustandsprüfung aus, für die Sie Details anzeigen möchten.
6. Wählen Sie im unteren Bereich die Registerkarte Health Checker aus.

> **Note**
>
> Neue Zustandsprüfungen müssen an Route 53-Zustandsprüfer verbreitet werden, bevor der Status der Zustandsprüfung und der letzte Grund für einen Ausfall in der Spalte Status angezeigt wird. Solange die Verbreitung nicht abgeschlossen ist, erklärt die Nachricht in der Spalte, dass kein Status verfügbar ist.

7. Die Tabelle enthält die folgenden Werte:

   Zustandsprüfer-IP

   Die IP-Adresse des Route 53-Zustandsprüfers, der die Zustandsprüfung durchführt.

   Letzte Überprüfung

   Datum und Uhrzeit der Integritätsprüfung oder Datum und Uhrzeit des letzten Fehlers.

   Status

   Entweder der aktuelle Status der Integritätsprüfung oder der Grund für das Fehlschlagen der letzten Integritätsprüfung.

Old console

Um den Status und den Grund für den letzten Fehler bei einer Integritätsprüfung anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Eine Übersicht über den Status Ihrer Zustandsprüfungen – fehlerfrei oder fehlerhaft – finden Sie in der Spalte Status. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.
4. Für alle Zustandsprüfungen mit Ausnahme von berechneten Zustandsprüfungen können Sie den Status der Route 53-Zustandsprüfer, die den Status eines angegebenen Endpunkts überprüfen, anzeigen. Wählen Sie die Zustandsprüfung aus.
5. Wählen Sie im unteren Bereich die Registerkarte Health Checkers aus.

   > **Note**
   >
   > Neue Zustandsprüfungen müssen an Route 53-Zustandsprüfer verbreitet werden, bevor der Status der Zustandsprüfung und der letzte Grund für einen Ausfall in der Spalte Status angezeigt wird. Solange die Verbreitung nicht abgeschlossen ist, erklärt die Nachricht in der Spalte, dass kein Status verfügbar ist.

6. Wählen Sie, ob Sie den aktuellen Status der Zustandsprüfung oder das Datum und die Uhrzeit des letzten Ausfalls und den Grund für den Ausfall anzeigen möchten. In der Tabelle auf der Registerkarte Status enthält die folgenden Werte:

   Zustandsprüfer-IP

   Die IP-Adresse des Route 53-Zustandsprüfers, der die Zustandsprüfung durchführt.

   Letzte Überprüfung

   Das Datum und die Uhrzeit der Zustandsprüfung oder das Datum und die Uhrzeit des letzten Ausfalls, abhängig von der Option, die Sie oben auf der Registerkarte Status auswählen.

   Status

   Entweder der aktuelle Status der Zustandsprüfung oder der Grund für den letzten Ausfall, abhängig von der Option, die Sie oben auf der Registerkarte Status auswählen.

Überwachung der Latenz zwischen Zustandsprüfern und Ihrem Endpunkt

Wenn Sie beim Erstellen einer Integritätsprüfung den Status eines Endpunkts (nicht den Status anderer Integritätsprüfungen) überwachen möchten und die Option Latenzdiagramme wählen, können Sie die folgenden Werte in CloudWatch Diagrammen auf der Route 53-Konsole anzeigen:

- Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen benötigten, um eine TCP-Verbindung mit dem Endpunkt herzustellen
- Die Durchschnittszeit in Millisekunden, bis die Route 53-Zustandsprüfungen die ersten Byte von einer Antwort auf eine HTTP- oder HTTPS-Anforderung erhalten haben
- Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen benötigten, um den SSL/TLS-Handshake abzuschließen

> **Note**
>
> Sie können die Latenzüberwachung nicht für vorhandene Zustandsprüfungen aktivieren.

> **Important**
>
> Die Zustandsprüfungen werden in 16 redundanten Availability Zones ausgeführt. Gelegentlich kann eine Availability Zone aufgrund von Bereitstellungen, Updates, Wartung usw. nicht verfügbar sein. Das System zur Gesundheitsprüfung ist darauf ausgelegt, dies ohne Auswirkungen auf den Kunden zu berücksichtigen.

> **Note**
>
> Wir aktualisieren die Health Checks-Konsole für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console

- Alte Konsole

New console

Um die Latenz zwischen Route 53-Zustandsprüfern und Ihrem Endpunkt anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID für die Zustandsprüfung aus, für die Sie Messwerte anzeigen möchten. Sie können Latenzdaten nur für Zustandsprüfungen anzeigen, die den Status eines Endpunkts überwachen, für den die Option Latency graphs aktiviert ist.
4. Wählen Sie im unteren Bereich die Registerkarte Metriken aus.
5. Wählen Sie den Zeitraum und die geografische Region aus, für die Sie Latenzdiagramme anzeigen möchten.

   Die Diagramme zeigen den Status für den angegebenen Zeitraum an:

   TCP-Verbindungszeit (nur HTTP und TCP)

   Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfer in der ausgewählten geografischen Region benötigten, um eine TCP-Verbindung mit dem Endpunkt herzustellen.

   Zeit bis zum ersten Byte (nur HTTP und HTTPS)

   Die Durchschnittszeit in Millisekunden, bis die Route 53-Zustandsprüfer in der ausgewählten geografischen Region die ersten Bytes einer Antwort auf eine HTTP- oder HTTPS-Anforderung erhalten haben.

   Zeit bis zum Abschluss des SSL-Handshake (nur HTTPS)

   Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen in der ausgewählten geografischen Region benötigten, um den SSL/TLS-Handshake abzuschließen.
6. Um ein größeres Diagramm anzuzeigen und andere Einstellungen festzulegen, wählen Sie die drei Punkte oben rechts im Diagramm aus. Sie können die folgenden Einstellungen ändern:

Statistik

Ändert die Berechnung, die CloudWatch mit den Daten durchgeführt wird.

Zeitraum

Zeigt den Status einer Zustandsprüfung über einen anderen Zeitraum an, z. B. über Nacht oder letzte Woche.

Intervall

Ändert das Intervall zwischen den Datenpunkten im Diagramm.

Beachten Sie Folgendes:

- Wenn Sie gerade eine Zustandsprüfung erstellt haben, kann es einige Minuten dauern, bis die grafische Darstellung der Daten erfolgt und die Metriken für die Zustandsprüfung in der Liste der verfügbaren Metriken angezeigt werden.
- Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol  .
- Wenn Zustandsprüfungen aus irgendeinem Grund fehlschlagen, z. B. wegen eines Verbindungs-Timeout oder weil Route 53 die Latenz nicht messen kann und Latenzdaten für den betroffenen Zeitraum im Diagramm fehlen werden.

Old console

Um die Latenz zwischen Route 53-Integritätsprüfern und Ihrem Endpunkt anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die Zeile für die entsprechenden Zustandsprüfungen. Sie können Latenzdaten nur für Zustandsprüfungen anzeigen, die den Status eines Endpunkts überwachen, für den die Option Latency graphs aktiviert ist.
4. Wählen Sie im unteren Bereich die Registerkarte Latency aus.

5. Wählen Sie den Zeitraum und die geografische Region aus, für die Sie Latenzdiagramme anzeigen möchten.

   Die Diagramme zeigen den Status für den angegebenen Zeitraum an:

   TCP-Verbindungszeit (nur HTTP und TCP)

   Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfer in der ausgewählten geografischen Region benötigten, um eine TCP-Verbindung mit dem Endpunkt herzustellen.

   Zeit bis zum ersten Byte (nur HTTP und HTTPS)

   Die Durchschnittszeit in Millisekunden, bis die Route 53-Zustandsprüfer in der ausgewählten geografischen Region die ersten Bytes einer Antwort auf eine HTTP- oder HTTPS-Anforderung erhalten haben.

   Zeit bis zum Abschluss des SSL-Handshake (nur HTTPS)

   Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen in der ausgewählten geografischen Region benötigten, um den SSL/TLS-Handshake abzuschließen.

   > **Note**
   >
   > Wenn Sie mehr als eine Zustandsprüfung auswählen, zeigt das Diagramm eine separate farbcodierte Zeile für jede Zustandsprüfung an.

6. Um das Diagramm zu vergrößern und andere Einstellungen festzulegen, klicken Sie auf das Diagramm. Sie können die folgenden Einstellungen ändern:

   Statistik

   Ändert die Berechnung, die CloudWatch mit den Daten durchgeführt wird.

   Zeitraum

   Zeigt den Status einer Zustandsprüfung über einen anderen Zeitraum an, z. B. über Nacht oder letzte Woche.

Intervall

Ändert das Intervall zwischen den Datenpunkten im Diagramm.

Beachten Sie Folgendes:

- Wenn Sie gerade eine Zustandsprüfung erstellt haben, kann es einige Minuten dauern, bis die grafische Darstellung der Daten erfolgt und die Metriken für die Zustandsprüfung in der Liste der verfügbaren Metriken angezeigt werden.
- Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol  .
- Wenn Zustandsprüfungen aus irgendeinem Grund fehlschlagen, z. B. wegen eines Verbindungs-Timeout oder weil Route 53 die Latenz nicht messen kann und Latenzdaten für den betroffenen Zeitraum im Diagramm fehlen werden.

Überwachung von Zustandsprüfungen mit CloudWatch

Route 53-Zustandsprüfungen sind in CloudWatch Metriken integriert, sodass Sie Folgendes tun können:

- Überprüfen Sie, ob eine Zustandsprüfung korrekt konfiguriert ist.
- Überprüfen Sie den Status einer Zustandsprüfung über einen festgelegten Zeitraum hinweg.
- Konfigurieren CloudWatch Sie so, dass eine Amazon SNS SNS-Warnung gesendet wird, wenn der Status einer Zustandsprüfung fehlerhaft ist. Beachten Sie, dass einige Minuten zwischen dem Zeitpunkt, zu dem eine Zustandsprüfung fehlschlägt, und dem Zeitpunkt, zu dem Sie die entsprechende SNS-Benachrichtigung erhalten, vergehen können.

Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Themen

- Sehen Sie sich den Status Ihres Gesundheitschecks an
- Alarme zur Gesundheitsprüfung anzeigen
- Sehen Sie sich die Metriken zur Gesundheitsprüfung auf der CloudWatch Konsole an

- Erstellen Sie einen Alarm mit einer SNS-Benachrichtigung

Sehen Sie sich den Status Ihres Gesundheitschecks an

> **Note**
>
> Wir aktualisieren die Konsole für Gesundheitschecks für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

Um den Status einer Zustandsprüfung einzusehen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die verknüpfte ID der Zustandsprüfung aus, für die Sie Messwerte anzeigen möchten.
4. Wählen Sie im unteren Bereich die Registerkarte Metriken aus.

   Die beiden Diagramme zeigen den Status der letzten Stunde in Intervallen von einer Minute an:

   Status der Zustandsprüfung

   Das Diagramm zeigt, wie Route 53 den Endpunkt bewertet.1zeigt, wie0zeigt, wie fehlerhaft.

Zustandsprüfer, die berichten, dass der Endpunkt fehlerfrei ist (%)

Für Zustandsprüfungen, bei denen nur ein Endpunkt überwacht wird, zeigt das Diagramm den Prozentsatz der Route 53-Zustandsprüfungen an, die den ausgewählten Endpunkt als fehlerfrei einstufen.

Wenn eine Zustandsprüfung deaktiviert ist, ist diese Metrik nicht verfügbar.

Anzahl der fehlerfreien untergeordneten Zustandsprüfungen

Nur für berechnete Zustandsprüfungen zeigt das Diagramm die Anzahl der untergeordneten Zustandsprüfungen an, die fehlerfrei sind.

5. Um ein größeres Diagramm anzuzeigen und andere Einstellungen festzulegen, wählen Sie die drei Punkte oben rechts und dann „Vergrößern“. Sie können die folgenden Einstellungen ändern:

   Statistik

   Ändert die Berechnung, die CloudWatch mit den Daten durchgeführt wird.

   Zeitraum

   Zeigt den Status einer Zustandsprüfung über einen anderen Zeitraum an, z. B. über Nacht oder letzte Woche.

   Intervall

   Ändert das Intervall zwischen den Datenpunkten im Diagramm.

   Beachten Sie Folgendes:

   - Wenn Sie gerade eine Zustandsprüfung erstellt haben, kann es einige Minuten dauern, bis die grafische Darstellung der Daten erfolgt und die Metriken für die Zustandsprüfung in der Liste der verfügbaren Metriken angezeigt werden.
   - Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol

     .

Old console

Um den Status einer Integritätsprüfung einzusehen (neue Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Health Checks aus.
3. Wählen Sie die Reihen für die entsprechenden Zustandsprüfungen aus.
4. Wählen Sie im unteren Bereich die Registerkarte Monitoring aus.

   Die beiden Diagramme zeigen den Status der letzten Stunde in Intervallen von einer Minute an:

   Status der Zustandsprüfung

   Das Diagramm zeigt, wie Route 53 den Endpunkt bewertet.1zeigt, wie0zeigt, wie fehlerhaft.

   Zustandsprüfer, die berichten, dass der Endpunkt fehlerfrei ist (%)

   Für Zustandsprüfungen, bei denen nur ein Endpunkt überwacht wird, zeigt das Diagramm den Prozentsatz der Route 53-Zustandsprüfungen an, die den ausgewählten Endpunkt als fehlerfrei einstufen.

   Wenn eine Zustandsprüfung deaktiviert ist, ist diese Metrik nicht verfügbar.

   Anzahl der fehlerfreien untergeordneten Zustandsprüfungen

   Nur für berechnete Zustandsprüfungen zeigt das Diagramm die Anzahl der untergeordneten Zustandsprüfungen an, die fehlerfrei sind.

   > **Note**
   >
   > Wenn Sie mehr als eine Zustandsprüfung ausgewählt haben, zeigt das Diagramm eine separate farbcodierte Zeile für jede Zustandsprüfung an.

5. Um das Diagramm zu vergrößern und andere Einstellungen festzulegen, klicken Sie auf das Diagramm. Sie können die folgenden Einstellungen ändern:

Statistik

Ändert die Berechnung, die CloudWatch mit den Daten durchgeführt wird.

Zeitraum

Zeigt den Status einer Zustandsprüfung über einen anderen Zeitraum an, z. B. über Nacht oder letzte Woche.

Intervall

Ändert das Intervall zwischen den Datenpunkten im Diagramm.

Beachten Sie Folgendes:

- Wenn Sie gerade eine Zustandsprüfung erstellt haben, kann es einige Minuten dauern, bis die grafische Darstellung der Daten erfolgt und die Metriken für die Zustandsprüfung in der Liste der verfügbaren Metriken angezeigt werden.
- Die Grafik wird nicht automatisch aktualisiert. Wählen Sie zum Aktualisieren der Anzeige das Symbol

.

Alarme zur Gesundheitsprüfung anzeigen

> **Note**
>
> Wir aktualisieren die Konsole für Gesundheitschecks für Route 53. Während der Übergangsphase können Sie weiterhin die alte Konsole verwenden.

Wählen Sie den Tab für die von Ihnen verwendete Konsole aus.

- New console
- Alte Konsole

New console

So zeigen Sie den CloudWatch Alarmstatus an und bearbeiten Alarme für Amazon Route 53

1. Wählen Sie im Navigationsbereich der Route 53-Konsole Health Checks aus.
2. Wählen Sie die verknüpfte ID der Zustandsprüfung aus, für die Sie die Alarme anzeigen möchten.
3. Wählen Sie auf der Detailseite unten auf der Seite den Tab Alarme aus.

   Die Alarmliste enthält alle Route 53-Alarme, die Sie für die ausgewählte Zustandsprüfung erstellt haben.

   In der Spalte State wird der aktuelle Status eines Alarms angezeigt:

   OK

   CloudWatch hat genügend Statistiken aus Route 53-Zustandsprüfungen gesammelt, um festzustellen, dass der Endpunkt den Alarmschwellenwert nicht erreicht.

   UNZUREICHENDE DATEN

   CloudWatch hat nicht genügend Statistiken gesammelt, um festzustellen, ob der Endpunkt den Alarmschwellenwert erreicht. Dies ist der erste Status eines neuen Alarms. Der Alarmstatus ändert sich auch in UNZUREICHENDE DATEN, wenn CloudWatch Messwerte nicht mehr verfügbar sind oder wenn Sie die Zustandsprüfung löschen, ohne den zugehörigen Alarm zu löschen.

   ALARM

   CloudWatch hat genügend Statistiken aus Route 53-Zustandsprüfungen gesammelt, um festzustellen, ob der Endpunkt den Alarmschwellenwert erreicht, und um eine Benachrichtigung an die angegebene E-Mail-Adresse zu senden.
4. Um einen Alarm in der CloudWatch Konsole anzuzeigen, die detailliertere Informationen zum Alarm enthält (z. B. einen Verlauf der Alarmaktualisierungen und Statusänderungen), wählen Sie den verknüpften Namen des Alarms. Sie können den Alarm auch auf der CloudWatch Konsole bearbeiten.
5. Um einen neuen CloudWatch Alarm auf der CloudWatch Konsole zu erstellen, wählen Sie CloudWatch Alarm erstellen. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch unter Suchen und Erstellen von empfohlenen Alarmen.

Old console

So zeigen Sie den CloudWatch Alarmstatus an und bearbeiten Alarme für Amazon Route 53

1. Wählen Sie im Navigationsbereich der Route 53-Konsole Health Checks aus.
2. Wählen Sie die Zeile für die Zustandsprüfung.
3. Klicken Sie im Detailbereich (wenn Sie x für Health Checks Selected (Ausgewählte Statusprüfungen) aktiviert haben) das richtige Caret-Zeichen ( )

   Die CloudWatch Alarmliste enthält alle Route 53-Alarme, die Sie mit dem aktuellen AWS Konto erstellt haben.

   In der Spalte State wird der aktuelle Status eines Alarms angezeigt:

   OK

   CloudWatch hat genügend Statistiken aus Route 53-Zustandsprüfungen gesammelt, um festzustellen, dass der Endpunkt den Alarmschwellenwert nicht erreicht.

   UNZUREICHENDE DATEN

   CloudWatch hat nicht genügend Statistiken gesammelt, um festzustellen, ob der Endpunkt den Alarmschwellenwert erreicht. Dies ist der erste Status eines neuen Alarms. Der Alarmstatus ändert sich auch in UNZUREICHENDE DATEN, wenn CloudWatch Messwerte nicht mehr verfügbar sind oder wenn Sie die Zustandsprüfung löschen, ohne den zugehörigen Alarm zu löschen.

   ALARM

   CloudWatch hat genügend Statistiken aus Route 53-Zustandsprüfungen gesammelt, um festzustellen, ob der Endpunkt den Alarmschwellenwert erreicht, und um eine Benachrichtigung an die angegebene E-Mail-Adresse zu senden.
4. Zum Anzeigen und Bearbeiten von Einstellungen für einen Alarm, wählen Sie den Namen des Alarms.
5. Um einen Alarm in der CloudWatch Konsole anzuzeigen, die detailliertere Informationen zum Alarm enthält (z. B. einen Verlauf der Alarmaktualisierungen und Statusänderungen), wählen Sie in der Spalte Weitere Optionen für den Alarm die Option Ansicht aus.

6. Um alle CloudWatch Alarme anzuzeigen, die Sie mit dem aktuellen AWS Konto erstellt haben, einschließlich Alarme für andere AWS Dienste, wählen Sie „Alle CloudWatch Alarme anzeigen“.
7. Um alle verfügbaren CloudWatch Messwerte anzuzeigen, einschließlich Messwerte, die derzeit nicht vom aktuellen AWS Konto verwendet werden, wählen Sie „Alle CloudWatch Metriken anzeigen“.

Sehen Sie sich die Metriken zur Gesundheitsprüfung auf der CloudWatch Konsole an

Um Route 53-Metriken auf der CloudWatch Konsole anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Ändern Sie die aktuelle Region inUSA Ost (Nord-Virginia)aus. Route 53-Metriken sind nicht verfügbar, wenn Sie eine andere Region als die aktuelle Region auswählen.
3. Wählen Sie im Navigationsbereich Metriken aus.
4. Klicken Sie auf der Registerkarte All metrics auf Route 53.
5. Wählen Sie Health Check Metrics.
6. Sie können die SNS-Benachrichtigung auch auf der CloudWatch Konsole einrichten. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch unter Empfohlene Alarme erstellen.

Erstellen Sie einen Alarm mit einer SNS-Benachrichtigung

> **Note**
>
> Das folgende Verfahren gilt nur für die alte Konsole. Die neue Konsole leitet Sie zur CloudWatch Konsole weiter, um Alarme zu erstellen. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch unter Suchen und Erstellen von empfohlenen Alarmen.

Um eine Amazon SNS SNS-Benachrichtigung zu erhalten, wenn der Status einer Zustandsprüfung fehlerhaft ist (alte Konsole)

1. Wählen Sie im Navigationsbereich der Route 53-Konsole Health Checks aus.

2. Wählen Sie die Zeile für die entsprechende Zustandsprüfung.
3. Klicken Sie im unteren Bereich auf die Registerkarte Alarms.

   In der Tabelle werden die Alarme aufgeführt, die Sie bereits für diese Zustandsprüfung erstellt haben.
4. Wählen Sie Alarm erstellen aus.
5. Geben Sie die folgenden Werte an:

   Name des Alarms

   Geben Sie in der Spalte Name den Namen ein, den Route 53 auf der Registerkarte Alarms (Alarme) anzeigen soll.

   Beschreibung des Alarms

   (Optional) Geben Sie eine Beschreibung für den Alarm ein. Dieser Wert wird in der CloudWatch Konsole angezeigt.

   Benachrichtigungen senden

   Wählen Sie aus, ob Route 53 Ihnen eine Benachrichtigungen senden soll, wenn der Status dieser Zustandsprüfung einen Alarm auslöst.

   Benachrichtigungsziel (nur, wenn für "Benachrichtigung senden" die Option "Ja" ausgewählt haben)

   Wenn Sie eine Benachrichtigung CloudWatch zu einem vorhandenen SNS-Thema senden möchten, wählen Sie das Thema aus der Liste aus.

   Wenn Sie eine Benachrichtigung CloudWatch , aber nicht an ein vorhandenes SNS-Thema senden möchten, gehen Sie wie folgt vor:

   - Wenn Sie eine E-Mail-Benachrichtigung senden CloudWatch möchten, wählen Sie Neues SNS-Thema und fahren Sie mit diesem Verfahren fort.
   - Wenn Sie Benachrichtigungen mit einer anderen Methode senden CloudWatch möchten, öffnen Sie einen neuen Browser-Tab, rufen Sie die Amazon SNS SNS-Konsole auf und erstellen Sie das neue Thema. Kehren Sie dann zur Route 53-Konsole zurück, wählen Sie den Namen des neuen Themas in der Liste Notification target (Benachrichtigungsziel) aus und setzen Sie den Vorgang fort.

Themenname (nur, wenn Sie ein neues Amazon-SNS-Thema erstellen möchten)

Geben Sie den Namen des neuen Amazon-SNS-Themas ein.

Empfänger-E-Mail-Adressen (nur, wenn Sie eine neues Amazon-SNS-Thema erstellen möchten)

Geben Sie die E-Mail-Adresse ein, an die Route 53 eine SNS-Benachrichtigung senden soll, wenn eine Zustandsprüfung einen Alarm auslöst.

Alarmziel

Wählen Sie den Wert aus, der von Route 53 für diese Zustandsprüfung ausgewertet werden soll:

- Health check status (Status der Gesundheitsprüfung) - Die Route 53-Zustandsprüfung meldet, dass die Zustandsprüfung ein fehlerfreies oder instabiles Ergebnis ermittelt hat.
- Health checkers that reports the endpoint healthy (%) (Zustandsprüfungen, die angeben, dass der Endpunkt fehlerfrei ist (%)) (Zustandsprüfungen, bei denen nur ein Endpunkt überwacht wird) Der Prozentsatz der Route 53-Zustandsprüfungen, die einen fehlerfreien Status ermittelt haben.
- Number of healthy child health checks (Anzahl der fehlerfreien untergeordneten Zustandsprüfungen) (nur berechnete Zustandsprüfungen) - Die Anzahl der untergeordneten Zustandsprüfungen in einer berechneten Zustandsprüfung, die melden, dass die Zustandsprüfung einen fehlerfreien Status ermittelt hat.
- TCP connection time (TCP-Verbindungszeit) (nur HTTP- und TCP-Zustandsprüfungen) - Die Zeit in Millisekunden, die die Route 53-Zustandsprüfung benötigt, um eine TCP-Verbindung mit dem Endpunkt herzustellen.
- Time to complete SSL handshake (Zeit bis zum Abschluss des SSL-Handshake) (nur HTTPS-Zustandsprüfungen) - Die Zeit in Millisekunden, die die Route 53-Zustandsprüfung für das SSL/TLS-Handshake benötigt.
- Time to first byte (Zeit zum ersten Byte) (nur HTTP- und HTTPS-Zustandsprüfungen) Die Zeit in Millisekunden, die die Route 53-Zustandsprüfungen benötigen, um das erste Antwort-Byte auf eine HTTP- oder HTTPS-Anforderung zu empfangen.

Alarmziel

Wählen Sie für die Alarmziele, die auf der Latenz (TCP-Verbindungszeit, Zeit bis zum Abschluss des SSL-Handshakes, Zeit bis zum ersten Byte) basieren, aus, ob Sie die Latenz für Route 53-Zustandsprüfungen in einer bestimmten Region oder für alle Regionen (global) berechnen möchtenCloudWatch .

Wenn Sie eine Region auswählen, misst Route 53 die Latenz nur zweimal pro Minute und die Anzahl der Stichproben ist kleiner, als wenn Sie alle Regionen auswählen. Daher sind Werte außerhalb der Bereiche wahrscheinlicher. Um falsche Alarmbenachrichtigungen zu vermeiden, empfehlen wir, dass Sie eine größere Anzahl aufeinander folgender Zeiträume festlegen, in denen die Zustandsprüfung fehlschlagen muss, bevor CloudWatch Ihnen eine Benachrichtigung sendet.

Bedingung erfüllen

Verwenden Sie die folgenden Einstellungen, um zu bestimmen, wann ein CloudWatch Alarm ausgelöst werden soll.

Alarmziel	Empfohlene Bedingung	Beschreibung
Status der Zustandsprüfung	Minimum < 1	Route 53-Zustandsprüfungen erstellen einen Bericht, wenn der Endpunkt fehlerhaft ist.
Zustandsprüfer, die berichten, dass der Endpunkt fehlerfrei ist (%)	Average (Durchschnitt) < gewünschter Prozentsatz	Zustandsprüfungen, bei denen nur ein Endpunkt überwacht wird - Route 53 betrachtet den Status einer Zustandsprüfung als fehlerhaft, wenn weniger als 18 % der Zustandsprüfungen den Status "fehlerfrei" melden. Wählen Sie für diese Metrik nicht Sample Count (Probenanzahl) aus, da sich der Bereich der Probenanzahl ändern kann, wenn Route 53 mehr Zustandsprüfungsregionen hinzufügt. Average (Durchschnitt) gibt immer den tatsächlichen Prozentsatz der Prüfungen wieder, die den Status einer Zustandsprüfung melden.

Alarmziel	Empfohlene Bedingung	Beschreibung
Anzahl der fehlerfreien untergeordneten Zustandsprüfungen	Minimum < Anzahl der fehlerfreien untergeordneten Zustandsprüfungen	Der Statistikwert Minimum gibt den konservativsten Wert zurück und stellt das Worst-Case-Szenario dar.
TCP connection time	Average > gewünschte Zeit in Millisekunden	Der Average ist ein konsistenterer Wert als andere Statistikwerte.
Time to complete SSL handshake	Average > gewünschte Zeit in Millisekunden	Der Average ist ein konsistenterer Wert als andere Statistikwerte.
Time to first byte	Average > gewünschte Zeit in Millisekunden	Der Average ist ein konsistenterer Wert als andere Statistikwerte.

Für mindestens ***x*** aufeinanderfolgende Zeiträume von ***y*** minutes/hours/day

Geben Sie die Anzahl der aufeinanderfolgenden Zeiträume an, in denen der angegebene Wert die Kriterien erfüllen muss, bevor Route 53 Benachrichtigungen sendet. Anschließend geben Sie die Länge des Zeitraums an.

6. Wenn Sie Create auswählen, sendet Amazon SNS Ihnen eine E-Mail mit Informationen zu dem neuen SNS-Thema.
7. Wählen Sie in der E-Mail Confirm subscription (Abonnement bestätigen). Sie müssen Ihr Abonnement bestätigen, um CloudWatch Benachrichtigungen zu erhalten.

Verwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr

Mit Resolver DNS Firewall können Sie ausgehenden DNS-Verkehr für Ihre Virtual Private Cloud (VPC) filtern und regulieren. Dazu erstellen Sie wiederverwendbare Sammlungen von Filterregeln in Regelgruppen der DNS-Firewall, ordnen die Regelgruppen Ihrer VPC zu und überwachen dann Aktivitäten in DNS-Firewall-Protokollen und -Metriken. Je nach Aktivität können Sie das Verhalten der DNS-Firewall entsprechend anpassen.

Die DNS-Firewall bietet Schutz für ausgehende DNS-Anfragen von Ihrem. VPCs Diese Anfragen werden zur Auflösung von Domainnamen über VPC Resolver weitergeleitet. Eine primäre Verwendung des DNS-Firewall-Schutzes besteht darin, die DNS-Exfiltration Ihrer Daten zu verhindern. Die DNS-Exfiltration kann auftreten, wenn ein schlechter Akteur eine Anwendungs-Instance in Ihrer VPC gefährdet und dann DNS-Lookup verwendet, um Daten aus der VPC an eine Domain zu senden, die sie steuern. Mit der DNS-Firewall können Sie die Domains überwachen und steuern, die Ihre Anwendungen abfragen können. Sie können den Zugriff auf die Domains verweigern, von denen Sie wissen, dass sie schlecht sind und alle anderen Abfragen durchlaufen können. Alternativ können Sie allen Domains den Zugriff verweigern, außer jenen, denen Sie explizit vertrauen.

Sie können die DNS-Firewall auch verwenden, um Auflösungsanforderungen an Ressourcen in privaten gehosteten Zonen (gemeinsam oder lokal) einschließlich VPC-Endpunktnamen zu blockieren. Es kann auch Anfragen für öffentliche oder private EC2 Amazon-Instanznamen blockieren.

Die DNS-Firewall ist eine Funktion von Route 53 VPC Resolver, für deren Verwendung kein zusätzliches VPC-Resolver-Setup erforderlich ist.

AWS Firewall Manager unterstützt die DNS-Firewall

Sie können den Firewall Manager verwenden, um Ihre DNS-Firewall-Regelgruppenzuordnungen für Ihre Konten in zentral VPCs zu konfigurieren und zu verwalten AWS Organizations. Firewall Manager fügt automatisch Verknüpfungen hinzu VPCs , die in den Geltungsbereich Ihrer Firewall Manager Manager-DNS-Firewall-Richtlinie fallen. Weitere Informationen finden Sie AWS Firewall Managerim Entwicklerhandbuch AWS WAF AWS Firewall Manager, und im AWS Shield Advanced Entwicklerhandbuch.

Wie funktioniert die DNS-Firewall mit AWS Network Firewall

Die DNS-Firewall und die Network Firewall bieten eine Filterung von Domainnamen, jedoch für verschiedene Arten von Datenverkehr. Zusammen mit DNS-Firewall und Network Firewall können Sie Domain-basierte Filterung für den Datenverkehr auf Anwendungsebene über zwei verschiedene Netzwerkpfade konfigurieren.

- Die DNS-Firewall bietet Filterung für ausgehende DNS-Abfragen, die den Route 53 VPC Resolver von Anwendungen in Ihrem. VPCs Sie können die DNS-Firewall auch so konfigurieren, dass benutzerdefinierte Antworten für Abfragen an blockierte Domainnamen gesendet werden.
- Die Network Firewall filtert sowohl den Datenverkehr auf Netzwerk- als auch auf Anwendungsebene, hat jedoch keinen Einblick in Abfragen, die vom Route 53 VPC Resolver gestellt wurden.

Weitere Informationen finden über Network Firewall im Network-Firewall-Entwicklerhandbuch.

So funktioniert die Resolver DNS Firewall

Mit der Resolver DNS Firewall können Sie den Zugriff auf Websites kontrollieren und Bedrohungen auf DNS-Ebene für DNS-Abfragen blockieren, die von Ihrer VPC über den Route 53 VPC Resolver ausgehen. Mit der DNS-Firewall definieren Sie Regeln für die Filterung von Domainnamen in Regelgruppen, die Sie Ihren eigenen zuordnen. VPCs Sie können Listen mit Domainnamen angeben, die zugelassen oder blockiert werden sollen, oder erweiterte Resolver-DNS-Firewall-Regeln, die Schutz vor DNS-Tunneling und auf dem Domänengenerierungsalgorithmus (DGA) basierenden Bedrohungen bieten. Sie können die Antworten auf die DNS-Abfragen, die Sie blockieren, anpassen. Bei Regeln, die eine Domänenliste enthalten, können Sie die Regel auch so anpassen, dass bestimmte Abfragetypen, wie z. B. MX-Einträge, durchgelassen werden.

Die DNS-Firewall filtert nur nach dem Domainnamen. Dieser Name wird nicht in eine IP-Adresse aufgelöst, die blockiert werden soll. Darüber hinaus filtert die DNS-Firewall den DNS-Verkehr, aber sie filtert keine anderen Protokolle auf Anwendungsebene wie HTTPS, SSH, TLS, FTP usw.

Komponenten und Einstellungen der Resolver DNS-Firewall

Sie verwalten die DNS-Firewall mit den folgenden zentralen Komponenten und Einstellungen.

DNS Firewall-Regelgruppe

Definiert eine benannte, wiederverwendbare Sammlung von DNS-Firewallregeln zum Filtern von DNS-Abfragen. Sie füllen die Regelgruppe mit den Filterregeln auf und ordnen der Regelgruppe

dann eine oder mehrere zu. VPCs Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, aktivieren Sie die DNS-Firewall-Filterung für die VPC. Wenn VPC Resolver dann eine DNS-Abfrage für eine VPC empfängt, der eine Regelgruppe zugeordnet ist, leitet VPC Resolver die Abfrage zur Filterung an die DNS-Firewall weiter.

Wenn Sie einer einzelnen VPC mehrere Regelgruppen zuordnen, geben Sie deren Verarbeitungsreihenfolge über die Prioritätseinstellung in jeder Zuordnung an. Die DNS-Firewall verarbeitet Regelgruppen für eine VPC ab der Einstellung der niedrigsten numerischen Priorität.

Weitere Informationen finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.

DNS-Firewall-Regel

Definiert eine Filterregel für DNS-Abfragen in einer DNS-Firewall-Regelgruppe. Jede Regel gibt eine Domänenliste oder einen DNS-Firewall-Schutz und eine Aktion für DNS-Abfragen an, deren Domänen den Domänenspezifikationen in der Regel entsprechen. Sie können zulassen (nur Regeln mit Domänenlisten), blockieren oder bei übereinstimmenden Abfragen eine Warnung ausgeben. In Regeln mit Domänenlisten können Sie auch Abfragetypen für die Domänen in der Liste angeben. Sie können beispielsweise einen MX-Abfragetyp für eine oder mehrere bestimmte Domänen blockieren oder zulassen. Sie können auch benutzerdefinierte Antworten für blockierte Abfragen definieren.

Bei DNS-Firewallregeln können Sie nur übereinstimmende Abfragen blockieren oder bei entsprechenden Abfragen eine Warnung ausgeben.

Jede Regel in einer Regelgruppe hat eine Prioritätseinstellung, die innerhalb der Regelgruppe eindeutig ist. Die DNS-Firewall verarbeitet die Regeln in einer Regelgruppe ab der niedrigsten numerischen Prioritätseinstellung.

DNS-Firewall-Regeln existieren nur im Kontext der Regelgruppe, in der sie definiert sind. Sie können eine Regel unabhängig von ihrer Regelgruppe nicht wiederverwenden oder darauf verweisen.

Weitere Informationen finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.

Domainliste

Definiert eine benannte, wiederverwendbare Sammlung von Domainspezifikationen für die Verwendung in der DNS-Filterung. Jede Regel in einer Regelgruppe benötigt eine einzige Domainliste. Sie können die Domains angeben, für die Sie den Zugriff zulassen möchten, die Domains, für die Sie den Zugriff verweigern möchten, oder eine Kombination aus beiden. Sie

können Ihre eigenen Domainlisten erstellen und Domainlisten verwenden, die für Sie AWS verwaltet werden.

Weitere Informationen finden Sie unter Domain-Listen von Resolver DNS Firewall.

Einstellung für die Domainumleitung (nur Domainlisten)

Mit der Einstellung für die Domänenumleitung können Sie eine DNS-Firewallregel so konfigurieren, dass alle Domänen in der DNS-Umleitungskette überprüft werden (Standard), z. B. CNAME, DNAME usw., oder nur die erste Domäne, und den Rest als vertrauenswürdig eingestuft werden. Wenn Sie die gesamte DNS-Umleitungskette überprüfen möchten, müssen Sie die nachfolgenden Domänen zu einer Domänenliste hinzufügen, die in der Regel auf ALLOW gesetzt ist. Wenn Sie die gesamte DNS-Umleitungskette überprüfen möchten, müssen Sie die nachfolgenden Domänen zu einer Domänenliste hinzufügen und die Aktion festlegen, die die Regel ausführen soll, entweder ALLOW, BLOCK oder ALERT.

Weitere Informationen finden Sie unter Regeleinstellungen in der DNS-Firewall.

Abfragetyp (nur Domänenlisten)

Mit der Einstellung für den Abfragetyp können Sie eine DNS-Firewallregel konfigurieren, um einen bestimmten DNS-Abfragetyp zu filtern. Wenn Sie keinen Abfragetyp auswählen, wird die Regel auf alle DNS-Abfragetypen angewendet. Beispielsweise möchten Sie möglicherweise alle Abfragetypen für eine bestimmte Domain blockieren, aber MX-Einträge zulassen.

Weitere Informationen finden Sie unter Regeleinstellungen in der DNS-Firewall.

DNS Firewall Erweiterter Schutz

Erkennt verdächtige DNS-Abfragen auf der Grundlage bekannter Bedrohungssignaturen in DNS-Abfragen. Jede Regel in einer Regelgruppe erfordert eine einzelne erweiterte DNS-Firewall-Schutzeinstellung. Sie können folgenden Schutz wählen:

- Algorithmen zur Domain-Generierung (DGAs)

  DGAs werden von Angreifern verwendet, um eine große Anzahl von Domains zu generieren, um Malware-Angriffe zu starten.

- DNS-Tunneling

  DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.

- Wörterbuch: DGA

Wörterbücher DGAs werden von Angreifern verwendet, um mithilfe von Wörterbuchwörtern Domains zu generieren, um der Entdeckung in der command-and-control Malware-Kommunikation zu entgehen.

In einer erweiterten DNS-Firewall-Regel können Sie wählen, ob eine Anfrage, die der Bedrohung entspricht, blockiert oder eine Warnung angezeigt werden soll. Die Algorithmen zum Schutz vor Bedrohungen werden von verwaltet und aktualisiert AWS.

Weitere Informationen finden Sie unter Resolver DNS Firewall Advanced.

Vertrauensschwellenwert (nur DNS Firewall Advanced-Schutz)

Der Vertrauensschwellenwert für den Schutz vor DNS-Bedrohungen. Sie müssen diesen Wert angeben, wenn Sie eine Regel für DNS Firewall Advanced erstellen. Die Werte für das Vertrauensniveau bedeuten:

- Hoch – Erkennt nur die am besten bestätigten Bedrohungen bei einer niedrigen Rate an falsch-positiven Alarmen.
- Mittel – Sorgt für ein ausgewogenes Verhältnis zwischen der Erkennung von Bedrohungen und falsch-positiven Alarmen.
- Niedrig – Bietet die höchste Erkennungsrate für Bedrohungen, erhöht jedoch auch die Zahl der falsch-positiven Fehlalarme.

Weitere Informationen finden Sie unter Regeleinstellungen in der DNS-Firewall.

Verknüpfung zwischen einer DNS-Firewall-Regelgruppe und einer VPC

Definiert einen Schutz für eine VPC mithilfe einer DNS-Firewall-Regelgruppe und aktiviert die VPC Resolver DNS-Firewall-Konfiguration für die VPC.

Wenn Sie einer einzelnen VPC mehrere Regelgruppen zuordnen, geben Sie deren Verarbeitungsreihenfolge über die Prioritätseinstellung in den Zuordnungen an. Die DNS-Firewall verarbeitet Regelgruppen für eine VPC ab der Einstellung der niedrigsten numerischen Priorität.

Weitere Informationen finden Sie unter Aktivierung des Resolver-DNS-Firewall-Schutzes für Ihre VPC.

DNS-Firewall-Konfiguration für eine VPC

Gibt an, wie VPC Resolver mit dem DNS-Firewall-Schutz auf VPC-Ebene umgehen soll. Diese Konfiguration gilt immer dann, wenn mindestens eine DNS-Firewall-Regelgruppe mit der VPC verknüpft ist.

Diese Konfiguration legt fest, wie Route 53 VPC Resolver Abfragen verarbeitet, wenn die DNS-Firewall sie nicht filtern kann. Wenn der VPC Resolver keine Antwort von der DNS-Firewall auf eine Anfrage erhält, schlägt das Schließen standardmäßig fehl und blockiert die Abfrage.

Weitere Informationen finden Sie unter Konfiguration der DNS-Firewall-VPC.

Überwachung der DNS-Firewall-Aktionen

Sie können Amazon verwenden CloudWatch , um die Anzahl der DNS-Abfragen zu überwachen, die nach DNS-Firewall-Regelgruppen gefiltert werden. CloudWatch sammelt und verarbeitet Rohdaten zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind.

Weitere Informationen finden Sie unter Überwachung von Resolver-DNS-Firewall-Regelgruppen mit Amazon CloudWatch.

Sie können Amazon verwenden EventBridge, einen serverlosen Service, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden, um skalierbare, ereignisgesteuerte Anwendungen zu erstellen.

Weitere Informationen finden Sie unter Verwaltung von Resolver-DNS-Firewall-Ereignissen mit Amazon EventBridge.

Wie filtert die Resolver DNS Firewall DNS-Abfragen

Wenn dem Route 53 VPC Resolver Ihrer VPC eine DNS-Firewall-Regelgruppe zugeordnet ist, wird der folgende Datenverkehr von der Firewall gefiltert:

- DNS-Abfragen, die ihren Ursprung in dieser VPC haben und über VPC-DNS geleitet werden.
- DNS-Abfragen, die über Resolver-Endpunkte von On-Premises-Ressourcen in dieselbe VPC geleitet werden, deren Resolver die DNS-Firewall zugeordnet hat.

Wenn die DNS-Firewall eine DNS-Abfrage empfängt, filtert sie die Abfrage anhand der von Ihnen konfigurierten Regelgruppen, Regeln und anderen Einstellungen und sendet die Ergebnisse zurück an VPC Resolver:

- Die DNS-Firewall wertet die DNS-Abfrage mithilfe der Regelgruppen aus, die der VPC zugeordnet sind, bis sie eine Übereinstimmung findet oder alle Regelgruppen ausschöpft. Die DNS-Firewall wertet die Regelgruppen in der Reihenfolge der Priorität aus, die Sie in der Zuordnung festgelegt haben, beginnend mit der niedrigsten numerischen Einstellung. Weitere Informationen erhalten

Sie unter DNS-Firewall-Regelgruppen und -Regeln und Aktivierung des Resolver-DNS-Firewall-Schutzes für Ihre VPC.

- Innerhalb jeder Regelgruppe bewertet die DNS-Firewall die DNS-Abfrage anhand der Domänenliste oder der erweiterten DNS-Firewall-Schutzmaßnahmen, bis eine Übereinstimmung gefunden wird oder alle Regeln ausgeschöpft sind. DNS-Firewall wertet die Regeln in der Reihenfolge ihrer Priorität aus, beginnend mit der niedrigsten numerischen Einstellung. Weitere Informationen finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.
- Wenn die DNS-Firewall eine Übereinstimmung mit der Domänenliste einer Regel oder Anomalien feststellt, die durch den erweiterten Regelschutz der DNS-Firewall identifiziert wurden, beendet sie die Abfrageauswertung und antwortet VPC Resolver mit dem Ergebnis. Wenn die Aktion aktiviert ist`alert`, sendet die DNS-Firewall auch eine Warnung an die konfigurierten VPC-Resolver-Protokolle. Weitere Informationen finden Sie unter Regelaktionen in der DNS-Firewall, Domain-Listen von Resolver DNS Firewall und Resolver DNS Firewall Advanced.
- Wenn die DNS-Firewall alle Regelgruppen auswertet, ohne eine Übereinstimmung zu finden, antwortet sie wie gewohnt auf die Abfrage.

VPC Resolver leitet die Anfrage entsprechend der Antwort der DNS-Firewall weiter. In dem unwahrscheinlichen Fall, dass die DNS-Firewall nicht reagiert, wendet VPC Resolver den konfigurierten DNS-Firewall-Fail-Modus der VPC an. Weitere Informationen finden Sie unter Konfiguration der DNS-Firewall-VPC.

Allgemeine Schritte zur Verwendung der Resolver DNS Firewall

Um die Resolver-DNS-Firewall-Filterung in Ihrer Amazon Virtual Private Cloud Cloud-VPC zu implementieren, führen Sie die folgenden allgemeinen Schritte aus.

- Definieren Sie Ihren Filteransatz, Ihre Domainlisten oder Ihre DNS-Firewall-Schutzmaßnahmen — Entscheiden Sie, wie Sie Abfragen filtern möchten, identifizieren Sie die Domain-Spezifikationen, die Sie benötigen, und definieren Sie die Logik, die Sie zur Auswertung von Abfragen verwenden werden. Sie können beispielsweise alle Abfragen zulassen, die in einer Liste bekannter fehlerhafter Domains enthalten sind. Oder Sie möchten das Gegenteil tun und alle Domains bis auf eine genehmigte Liste blockieren, was als Walled-Garden-Ansatz bekannt ist. Sie können Ihre eigenen Listen mit genehmigten oder gesperrten Domainspezifikationen erstellen und verwalten und Sie können Domainlisten verwenden, die für Sie AWS verwaltet werden. Um Ihre DNS-Firewall-Einstellungen zu schützen, können Sie die Abfragen filtern, indem Sie sie alle blockieren, oder Sie können bei verdächtigem Abfrageverkehr an Domänen, der möglicherweise Anomalien im

Zusammenhang mit Bedrohungen (DGA, DNS-Tunneling, Dictionary-DGA) enthält, warnen, um Ihre DNS-Firewall-Einstellungen zu testen. Weitere Informationen erhalten Sie unter Domain-Listen von Resolver DNS Firewall und Resolver DNS Firewall Advanced.

- Erstellen einer Firewall-Regelgruppe – Erstellen Sie in der DNS-Firewall eine Regelgruppe zum Filtern von DNS-Abfragen für Ihre VPC. Sie müssen eine Regelgruppe in jeder Region erstellen, in der Sie sie verwenden möchten. Möglicherweise möchten Sie Ihr Filterverhalten auch in mehrere Regelgruppen unterteilen, um die Wiederverwendbarkeit in mehreren Filterszenarien für Ihre verschiedenen zu gewährleisten. VPCs Informationen zu Regelgruppen finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.
- Regeln hinzufügen und konfigurieren – Fügen Sie Ihrer Regelgruppe für jede Domainliste und jedes Filterverhalten, das die Regelgruppe bereitstellen soll, eine Regel hinzu. Legen Sie die Prioritätseinstellungen für Ihre Regeln so fest, dass sie innerhalb der Regelgruppe in der richtigen Reihenfolge verarbeitet werden, und geben Sie der Regel, die Sie zuerst auswerten möchten, die niedrigste Priorität. Informationen zu Regeln finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.
- Ordnen Sie die Regelgruppe Ihrer VPC zu – Ordnen Sie diese Ihrer VPC zu, um Ihre DNS-Firewall-Regelgruppe zu verwenden. Wenn Sie mehr als eine Regelgruppe für Ihre VPC verwenden, legen Sie die Priorität jeder Zuordnung so fest, dass die Regelgruppen in der richtigen Reihenfolge verarbeitet werden. Geben Sie der Regelgruppe, die Sie zuerst auswerten möchten, die niedrigste Priorität. Weitere Informationen finden Sie unter Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten.
- (Optional) Ändern Sie die Firewallkonfiguration für die VPC — Wenn Sie möchten, dass Route 53 VPC Resolver Abfragen blockiert, wenn die DNS-Firewall keine Antwort für sie zurücksendet, ändern Sie in VPC Resolver die DNS-Firewall-Konfiguration der VPC. Weitere Informationen finden Sie unter Konfiguration der DNS-Firewall-VPC.

Verwendung von Resolver-DNS-Firewall-Regelgruppen in mehreren Regionen

Die Resolver DNS Firewall ist ein regionaler Dienst, sodass Objekte, die Sie in einer AWS Region erstellen, nur in dieser Region verfügbar sind. Wenn Sie dieselbe Regelgruppe in mehr als einer Region verwenden möchten, müssen Sie die Regelgruppe in allen Regionen erstellen.

Das AWS Konto, das eine Regelgruppe erstellt hat, kann sie mit anderen AWS Konten gemeinsam nutzen. Weitere Informationen finden Sie unter Resolver-DNS-Firewall-Regelgruppen zwischen Konten teilen AWS.

Regionale Verfügbarkeit für die Resolver DNS Firewall

Die DNS-Firewall ist in den folgenden Versionen verfügbar: AWS-Regionen

- Afrika (Kapstadt)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Malaysia)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Region Asien-Pazifik (Osaka)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Thailand)
- Asien-Pazifik (Tokio)
- Region Kanada (Zentral)
- Kanada West (Calgary)
- Region Europa (Frankfurt)
- Region Europa (Irland)
- Region Europa (London)
- Europa (Milan)
- Region Europa (Paris)
- Europa (Spain)
- Europa (Stockholm)
- Europa (Zürich)
- Israel (Tel Aviv)
- Mexiko (Zentral)
- Middle East (Bahrain)

- Naher Osten (VAE)
- Südamerika (São Paulo)
- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- China (Peking)
- China (Ningxia)
- AWS GovCloud (US)

Erste Schritte mit der Resolver DNS Firewall

Die DNS-Firewall-Konsole enthält einen Assistenten, der Sie durch die folgenden Schritte für die ersten Schritte mit DNS Firewall führt:

- Erstellen Sie Regelgruppen für jeden Satz von Regeln, den Sie verwenden möchten.
- Füllen Sie für jede Regel die Domainliste aus, auf die Sie überprüfen möchten. Sie können Ihre eigenen Domainlisten erstellen und AWS verwaltete Domainlisten verwenden.
- Ordnen Sie Ihre Regelgruppen VPCs denen zu, in denen Sie sie verwenden möchten.

Beispiel für Resolver DNS Firewall, Walled Garden

In diesem Lernprogramm erstellen Sie eine Regelgruppe, die alle außer einer ausgewählten Gruppe von Domains blockiert, denen Sie vertrauen. Dies wird als geschlossene Plattform oder ummauerte Gartenansatz bezeichnet.

So konfigurieren Sie eine DNS-Firewall-Regelgruppe mit dem Konsolenassistenten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie mit Schritt 3 fort.

   - ODER -

Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die

die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.

2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie auf der Seite Regelgruppen die Option Regelgruppe hinzufügen aus.
5. Geben Sie für den Regelgruppennamen **`WalledGardenExample`** ein.

   Im Abschnitt Tags können Sie optional ein Schlüssel-Wert-Paar für ein Tag eingeben. Tags helfen Ihnen bei der Organisation und Verwaltung Ihrer AWS -Ressourcen. Weitere Informationen finden Sie unter Amazon-Route-53-Ressourcen-Markierung.
6. Wählen Sie Regelgruppe hinzufügen aus.
7. Wählen Sie auf der WalledGardenExampleDetailseite die Registerkarte Regeln und dann Regel hinzufügen aus.
8. Geben Sie im Bereich Regeldetails den Regelnamen **`BlockAll`** ein.
9. Wählen Sie im Bereich Domainliste Eigene Domainliste hinzufügen aus.
10. Wählen Sie unter Neue Domainliste auswählen oder erstellen die Option Neue Domainliste erstellen aus.
11. Geben Sie einen Namen **`AllDomains`** für die Domainliste ein und geben Sie dann in das Textfeld Geben Sie eine Domäne pro Zeile ein Sternchen ein: **`*`** ein.
12. Akzeptieren Sie für die Einstellung „Domainumleitung“ die Standardeinstellung und lassen Sie „Abfragetyp — optional“ leer.
13. Wählen Sie für die Aktion BLOCKIEREN aus und belassen Sie dann für die zu sendende Antwort die Standardeinstellung NODATA.
14. Wählen Sie Regel hinzufügen aus. Ihre Regel BlockAllwird auf der WalledGardenExampleSeite auf der Registerkarte Regeln angezeigt.
15. Wählen Sie auf der WalledGardenExampleSeite Regel hinzufügen aus, um Ihrer Regelgruppe eine zweite Regel hinzuzufügen.
16. Geben Sie im Bereich Regeldetails den Regelnamen ein **`AllowSelectDomains`**.
17. Wählen Sie im Bereich Domainliste Eigene Domainliste hinzufügen aus.
18. Wählen Sie unter Neue Domainliste auswählen oder erstellen die Option Neue Domainliste erstellen aus.

19. Geben Sie einen Domainlistennamen **`ExampleDomains`** ein.
20. Geben Sie in das Textfeld Eine Domäne pro Zeile eingeben in der ersten Zeile **`example.com`** und in der zweiten Zeile Folgendes ein**`example.org`**.

    > **Note**
    >
    > Wenn die Regel auch für Subdomains gelten soll, müssen Sie diese Domains ebenfalls zur Liste hinzufügen. Um beispielsweise alle Subdomains von example.com hinzuzufügen, fügen Sie **`*.example.com`** zur Liste hinzu.

21. Akzeptieren Sie für die Einstellung Domainumleitung die Standardeinstellung und lassen Sie Abfragetyp — optional leer.
22. Wählen Sie für die Aktion die Option ZULASSEN aus.
23. Wählen Sie Regel hinzufügen aus. Ihre Regeln werden beide auf der Registerkarte Regeln auf der WalledGardenExampleSeite angezeigt.
24. Auf der Registerkarte Regeln auf der WalledGardenExampleSeite können Sie die Bewertungsreihenfolge der Regeln in Ihrer Regelgruppe anpassen, indem Sie die in der Spalte Priorität aufgeführte Zahl auswählen und eine neue Zahl eingeben. Die DNS-Firewall bewertet Regeln ab der niedrigsten Prioritätseinstellung, sodass die Regel mit der niedrigsten Priorität als Erstes bewertet wird. In diesem Beispiel soll die DNS-Firewall zunächst DNS-Abfragen für die ausgewählte Liste der Domains identifizieren und zulassen und dann alle verbleibenden Abfragen blockieren.

    Passen Sie die Regelpriorität so an, dass die Regel eine niedrigere Priorität AllowSelectDomainshat.

Sie haben jetzt eine Regelgruppe, die nur bestimmte Domainabfragen zulässt. Um mit der Verwendung zu beginnen, ordnen Sie es VPCs dem Bereich zu, in dem Sie das Filterverhalten verwenden möchten. Weitere Informationen finden Sie unter Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten.

Beispiel für eine Resolver-DNS-Firewall-Sperrliste

In diesem Lernprogramm erstellen Sie eine Regelgruppe, die Domains blockiert, von denen Sie wissen, dass sie bösartig sind. Sie fügen außerdem einen DNS-Abfragetyp hinzu, der für die Domänen in der Sperrliste zulässig ist. Die Regelgruppe erlaubt alle anderen ausgehenden DNS-Anfragen über den VPC Resolver.

So konfigurieren Sie eine DNS-Firewall-Blockliste mithilfe des Konsolenassistenten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie mit Schritt 3 fort.

   - ODER -

   Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie auf der Seite Regelgruppen die Option Regelgruppe hinzufügen aus.
5. Geben Sie für den Regelgruppennamen **`BlockListExample`** ein.

   Im Abschnitt Tags können Sie optional ein Schlüssel-Wert-Paar für ein Tag eingeben. Tags helfen Ihnen bei der Organisation und Verwaltung Ihrer AWS -Ressourcen. Weitere Informationen finden Sie unter Amazon-Route-53-Ressourcen-Markierung.
6. Wählen Sie auf der BlockListExampleDetailseite die Registerkarte Regeln und dann Regel hinzufügen aus.
7. Geben Sie im Bereich Regeldetails den Regelnamen **`BlockList`** ein.
8. Wählen Sie im Bereich Domainliste Eigene Domainliste hinzufügen aus.
9. Wählen Sie unter Neue Domainliste auswählen oder erstellen die Option Neue Domainliste erstellen aus.
10. Geben Sie einen Domainlistennamen **`MaliciousDomains`** ein, und geben Sie dann in das Textfeld die Domains ein, die Sie blockieren möchten. Beispiel, **`example.org`**. Geben Sie pro Zeile eine Domain ein.

> **Note**
>
> Wenn die Regel auch auf Subdomains angewendet werden soll, müssen Sie diese Domains auch zur Liste hinzufügen. Um beispielsweise alle Subdomains von example.org hinzuzufügen, fügen Sie **`*.example.org`** zur Liste hinzu.

11. Akzeptieren Sie für die Einstellung Domainumleitung die Standardeinstellung und lassen Sie „Abfragetyp — optional“ leer.
12. Wählen Sie für die Aktion BLOCK aus und belassen Sie dann die zu sendende Antwort auf der Standardeinstellung von NODATA.
13. Wählen Sie Regel hinzufügen aus. Ihre Regel wird auf der Seite auf der BlockListExampleRegisterkarte Regeln angezeigt
14. Auf der Registerkarte Regeln auf der BlockedListExampleSeite können Sie die Reihenfolge der Auswertung der Regeln in Ihrer Regelgruppe anpassen, indem Sie die in der Spalte Priorität aufgeführte Zahl auswählen und eine neue Zahl eingeben. Die DNS-Firewall bewertet Regeln ab der niedrigsten Prioritätseinstellung, sodass die Regel mit der niedrigsten Priorität als Erstes bewertet wird.

    Wählen Sie die Regelpriorität aus und passen Sie sie an, sodass sie entweder vor oder nach allen anderen Regeln, die Sie haben, bewertet BlockListwird. Meistens sollten bekannte bösartige Domains zuerst blockiert werden. Das heißt, die damit verbundenen Regeln sollten die niedrigste Prioritätsnummer haben.
15. Um eine Regel hinzuzufügen, die MX-Einträge für die BlockList Domains zulässt, wählen Sie auf der BlockedListExampleDetailseite auf der Registerkarte Regeln die Option Regel hinzufügen aus.
16. Geben Sie im Bereich Regeldetails den Regelnamen **`BlockList-allowMX`** ein.
17. Wählen Sie im Bereich Domainliste Eigene Domainliste hinzufügen aus.
18. Wählen Sie unter Neue Domainliste auswählen oder erstellen die Option aus **`MaliciousDomains`**.
19. Akzeptieren Sie für die Einstellung Domainumleitung die Standardeinstellung.
20. Wählen Sie in der Liste DNS-Abfragetyp die Option MX: Spezifiziert Mailserver aus.
21. Wählen Sie für die Aktion die Option ZULASSEN.
22. Wählen Sie Regel hinzufügen aus.
23. Auf der Registerkarte Regeln auf der BlockedListExampleSeite können Sie die Reihenfolge der Auswertung der Regeln in Ihrer Regelgruppe anpassen, indem Sie die in der Spalte Priorität aufgeführte Zahl auswählen und eine neue Zahl eingeben. Die DNS-Firewall bewertet Regeln ab der niedrigsten Prioritätseinstellung, sodass die Regel mit der niedrigsten Priorität als Erstes bewertet wird.

    Wählen Sie die Regelpriorität aus und passen Sie sie an, sodass BlockList-allowMX entweder vor oder nach allen anderen Regeln, die Sie haben, ausgewertet wird. Da Sie MX-Abfragen

zulassen möchten, stellen Sie sicher, dass die Regel BlockList-allowMX eine niedrigere Priorität als hat. BlockList

Sie haben jetzt eine Regelgruppe, die bestimmte bösartige Domainabfragen blockiert, aber einen bestimmten DNS-Abfragetyp zulässt. Um mit der Verwendung zu beginnen, ordnen Sie es VPCs dem Bereich zu, in dem Sie das Filterverhalten verwenden möchten. Weitere Informationen finden Sie unter Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten.

DNS-Firewall-Regelgruppen und -Regeln

In diesem Abschnitt werden die Einstellungen beschrieben, die Sie für Ihre DNS-Firewall-Regelgruppen und -Regeln konfigurieren können, um das Verhalten der DNS-Firewall für Sie zu definieren VPCs. Außerdem wird beschrieben, wie Sie die Einstellungen für Ihre Regelgruppen und Regeln verwalten.

Wenn Sie Ihre Regelgruppen nach Ihren Wünschen konfiguriert haben, verwenden Sie sie direkt und können sie zwischen Konten und in Ihrer gesamten Organisation in AWS Organizations freigeben und verwalten.

- Sie können eine Regelgruppe mehreren zuordnen VPCs, um ein einheitliches Verhalten in Ihrer gesamten Organisation zu gewährleisten. Weitere Informationen finden Sie unter Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten.
- Sie können Regelgruppen für Konten freigeben, um eine konsistente DNS-Abfrageverwaltung in Ihrer gesamten Organisation zu gewährleisten. Weitere Informationen finden Sie unter Resolver-DNS-Firewall-Regelgruppen zwischen Konten teilen AWS.
- Sie können Regelgruppen in Ihrer gesamten Organisation verwenden, AWS Organizations indem Sie sie in AWS Firewall Manager Richtlinien verwalten. Informationen zu Firewall Manager finden Sie AWS Firewall Managerim AWS Shield Advanced Entwicklerhandbuch AWS WAF AWS Firewall Manager, und unter.

Regelgruppeneinstellungen in der DNS-Firewall

Wenn Sie eine DNS-Firewall-Regelgruppe erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Name

Ein eindeutiger Name, mit dem Sie ganz einfach eine Regelgruppe auf dem Dashboard finden können.

(Optionale) Beschreibung

Eine kurze Beschreibung, die mehr Kontext für die Regelgruppe bietet.

Region

Die AWS Region, die Sie bei der Erstellung der Regelgruppe ausgewählt haben. Eine Regelgruppe, die Sie in einer Region erstellen, ist nur in dieser Region verfügbar. Wenn Sie dieselbe Regelgruppe in mehr als einer Region verwenden möchten, müssen Sie die Regelgruppe in allen Regionen erstellen.

Regeln

Das Filterverhalten der Regelgruppe ist in den Regeln enthalten. Weitere Informationen finden Sie im folgenden Abschnitt.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Dies sind die Tags, mit AWS Fakturierung und Kostenmanagement denen Sie Ihre AWS Rechnung organisieren können. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing - Benutzerhandbuch.

Regeleinstellungen in der DNS-Firewall

Wenn Sie eine Regel in einer DNS-Firewall-Regelgruppe erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Name

Eine eindeutige ID für die Regel in der Regelgruppe.

(Optionale) Beschreibung

Eine kurze Beschreibung, die weitere Informationen über die Regel enthält.

Domainliste

Die Liste der Domains, auf die die Regel überprüft. Sie können Ihre eigene Domainliste erstellen und verwalten oder eine Domainliste abonnieren, die AWS für Sie verwaltet. Weitere Informationen finden Sie unter Domain-Listen von Resolver DNS Firewall.

Eine Regel kann entweder eine Domainliste oder einen erweiterten DNS-Firewall-Schutz enthalten, aber nicht beides.

Einstellung für die Domänenumleitung (nur Domänenlisten)

Sie können festlegen, dass die DNS-Firewallregel nur die erste Domäne oder alle (Standard) Domänen in der DNS-Umleitungskette überprüft, z. B. CNAME, DNAME usw. Wenn Sie sich dafür entscheiden, alle Domänen zu überprüfen, müssen Sie die nachfolgenden Domänen in der DNS-Umleitungskette zur Domänenliste hinzufügen und die Aktion festlegen, die die Regel ausführen soll, entweder ALLOW, BLOCK oder ALERT. Weitere Informationen finden Sie unter Komponenten und Einstellungen der Resolver DNS-Firewall.

Abfragetyp (nur Domänenlisten)

Die Liste der DNS-Abfragetypen, nach denen die Regel sucht. Die folgenden Werte sind gültig:

- A: Gibt eine IPv4 Adresse zurück.
- AAAA: Gibt eine IPv6-Adresse zurück.
- CAA: Einschränkungen, die SSL/TLS Zertifizierungen für CAs die Domain erstellen können.
- CNAME: Gibt einen anderen Domainnamen zurück.
- DS: Datensatz, der den DNSSEC-Signaturschlüssel einer delegierten Zone identifiziert.
- MX: Spezifiziert Mailserver.
- NAPTR: Regular-expression-based Umschreiben von Domainnamen.
- NS: Autorisierende Nameserver.
- PTR: Ordnet eine IP-Adresse einem Domainnamen zu.
- SOA: Beginn des Autoritätsdatensatzes für die Zone.
- SPF: Listet die Server auf, die berechtigt sind, E-Mails von einer Domain aus zu versenden.
- SRV: Anwendungsspezifische Werte, die Server identifizieren.
- TXT: Überprüft E-Mail-Absender und anwendungsspezifische Werte.
- Ein Abfragetyp, den Sie mithilfe der DNS-Typ-ID definieren, z. B. 28 für AAAA. Die Werte müssen als TYPE definiert sein *NUMBER*, wobei sie beispielsweise 1-65334 lauten *NUMBER* können. TYPE28 Weitere Informationen finden Sie unter Liste der DNS-Eintragstypen.

Sie können einen Abfragetyp pro Regel erstellen.

> **Note**
>
> Wenn Sie eine Firewall-BLOCKregel mit der Aktion NXDOMAIN für den Abfragetyp AAAA einrichten, wird diese Aktion nicht auf synthetische IPv6 Adressen angewendet, die generiert werden, wenn sie DNS64 aktiviert ist.

DNS Firewall Erweiterter Schutz

Erkennt verdächtige DNS-Abfragen auf der Grundlage bekannter Bedrohungssignaturen in DNS-Abfragen. Sie können zwischen folgenden Schutzoptionen wählen:

- Algorithmen zur Domain-Generierung (DGAs)

  DGAs werden von Angreifern verwendet, um eine große Anzahl von Domains zu generieren, um Malware-Angriffe zu starten.

- DNS-Tunneling

  DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.

- Wörterbuch: DGA

  Wörterbücher DGAs werden von Angreifern verwendet, um mithilfe von Wörterbuchwörtern Domains zu generieren, um der Entdeckung in der command-and-control Malware-Kommunikation zu entgehen.

In einer erweiterten DNS-Firewall-Regel können Sie wählen, ob eine Anfrage, die der Bedrohung entspricht, blockiert oder eine Warnung angezeigt werden soll.

Weitere Informationen finden Sie unter Resolver DNS Firewall Advanced.

Eine Regel kann entweder einen erweiterten DNS-Firewall-Schutz oder eine Domänenliste enthalten, aber nicht beides.

Vertrauensschwellenwert (nur DNS Firewall Advanced)

Der Vertrauensschwellenwert für DNS Firewall Advanced. Sie müssen diesen Wert angeben, wenn Sie eine Regel für DNS Firewall Advanced erstellen. Die Werte für das Vertrauensniveau bedeuten:

- Hoch – Erkennt nur die am besten bestätigten Bedrohungen bei einer niedrigen Rate an falsch-positiven Alarmen.
- Mittel – Sorgt für ein ausgewogenes Verhältnis zwischen der Erkennung von Bedrohungen und falsch-positiven Alarmen.
- Niedrig – Bietet die höchste Erkennungsrate für Bedrohungen, erhöht jedoch auch die Zahl der falsch-positiven Fehlalarme.

Weitere Informationen finden Sie unter Regeleinstellungen in der DNS-Firewall.

Action

Wie Sie möchten, dass die DNS-Firewall eine DNS-Abfrage verarbeitet, deren Domainname mit den Spezifikationen in der Domainliste der Regel übereinstimmt. Weitere Informationen finden Sie unter Regelaktionen in der DNS-Firewall.

Priorität

Eindeutige positive Ganzzahleinstellung für die Regel innerhalb der Regelgruppe, die die Verarbeitungsreihenfolge bestimmt. DNS-Firewall überprüft DNS-Abfragen anhand der Regeln in einer Regelgruppe beginnend mit der niedrigsten Prioritätseinstellung. Sie können die Priorität einer Regel jederzeit ändern, z. B. um die Reihenfolge der Verarbeitung zu ändern oder Platz für andere Regeln zu schaffen.

Regelaktionen in der DNS-Firewall

Wenn die DNS-Firewall eine Übereinstimmung zwischen einer DNS-Abfrage und einer Domainspezifikation in einer Regel findet, wendet sie die in der Regel angegebene Aktion auf die Abfrage an.

Sie müssen in jeder von Ihnen erstellten Regel eine der folgenden Optionen angeben:

- Allow— Beenden Sie die Überprüfung der Abfrage und lassen Sie sie durchgehen. Nicht verfügbar für DNS Firewall Advanced.
- Alert— Beenden Sie die Überprüfung der Abfrage, lassen Sie sie durchlaufen und protokollieren Sie eine Warnung für die Abfrage in den Route 53 VPC Resolver-Protokollen.
- Block— Unterbrechen Sie die Überprüfung der Abfrage, verhindern Sie, dass sie zum vorgesehenen Ziel weitergeleitet wird, und protokollieren Sie die Blockaktion für die Abfrage in den Route 53 VPC Resolver-Protokollen.

Antworten Sie mit der konfigurierten Blockantwort wie folgt:

- NODATA— Antwortet und gibt an, dass die Abfrage erfolgreich war, aber keine Antwort darauf verfügbar ist.
- NXDOMAIN— Antwortet und gibt an, dass der Domainname der Anfrage nicht existiert.
- OVERRIDE— Geben Sie in der Antwort eine benutzerdefinierte Überschreibung an. Diese Option erfordert die folgenden zusätzlichen Einstellungen:
  - Record value— Der benutzerdefinierte DNS-Eintrag, der als Antwort auf die Anfrage zurückgesendet werden soll.
  - Record type— Der Typ des DNS-Eintrags. Dies bestimmt das Format des Datensatzwertes. Dies muss `CNAME` lauten.
  - Time to live in seconds— Die empfohlene Zeitspanne für den DNS-Resolver oder Webbrowser, um den Override-Eintrag zwischenzuspeichern und ihn als Antwort auf diese Anfrage zu verwenden, falls er erneut empfangen wird. Standardmäßig ist dies Null, und der Datensatz wird nicht zwischengespeichert.

Weitere Informationen zur Konfiguration und zum Inhalt der Abfrageprotokolle finden Sie unter Abfrageprotokollierung und Werte, die in den VPC Resolver-Abfrageprotokollen erscheinen.

Verwenden Sie Alert, um die Blockierungsregeln zu testen

Wenn Sie eine Blockierungsregel zum ersten Mal erstellen, können Sie sie testen, indem Sie sie mit der auf Alert festgelegten Aktion konfigurieren. Sie können sich dann die Anzahl der Abfragen ansehen, bei denen die Regel eine Warnung ausgibt, um zu sehen, wie viele blockiert würden, wenn Sie die Aktion auf Block festlegen.

Regelgruppen und Regeln in der DNS-Firewall verwalten

Folgen Sie den Anweisungen in diesem Abschnitt, um Regelgruppen und Regeln in der Konsole zu verwalten.

Wenn Sie Änderungen an DNS-Firewall-Entitäten wie Regeln und Domainlisten vornehmen, werden die Änderungen überall dort weitergegeben, wo die Entitäten gespeichert und verwendet werden. Ihre Änderungen werden innerhalb von Sekunden angewendet, es kann jedoch zu einer kurzen Inkonsistenzzeit kommen, wenn die Änderungen an einigen Stellen und nicht an anderen Stellen eingetroffen sind. Wenn Sie beispielsweise eine Domain zu einer Domainliste hinzufügen, auf die durch eine Sperrregel verwiesen wird, wird die neue Domain möglicherweise kurz in einem Bereich

Ihrer VPC blockiert, während sie in einem anderen Bereich weiterhin zulässig ist. Diese temporäre Inkonsistenz kann auftreten, wenn Sie die Regelgruppe und VPC-Zuordnungen zum ersten Mal konfigurieren und vorhandene Einstellungen ändern. Im Allgemeinen dauern alle Inkonsistenzen dieses Typs nur wenige Sekunden.

Erstellen einer Regelgruppe und -regeln

Gehen Sie wie in diesem Verfahren beschrieben vor, um eine Regelgruppe zu erstellen und ihr Regeln hinzuzufügen.

So erstellen Sie eine Regelgruppe und ihre Regeln

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie mit Schritt 3 fort.

   - ODER -

   Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die Seite .

   die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie Regelgruppe hinzufügen und befolgen Sie dann die Anweisungen des Assistenten, um Ihre Regelgruppe und Regeleinstellungen anzugeben.

   Informationen zu den Werten für Regelgruppen finden Sie unter Regelgruppeneinstellungen in der DNS-Firewall.

   Informationen zu den Werten für Regeln finden Sie unter Regeleinstellungen in der DNS-Firewall.

Anzeigen und Aktualisieren einer Regelgruppe und Regeln

Gehen Sie wie folgt vor, um die Regelgruppen und die ihnen zugewiesenen Regeln anzuzeigen. Sie können auch die Regelgruppe und die Regeleinstellungen aktualisieren.

So zeigen Sie eine Regelgruppe an und aktualisieren sie

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie mit Schritt 3 fort.

   - ODER -

   Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die Seite .

   die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie die Regelgruppe aus, die Sie anzeigen oder bearbeiten möchten, und wählen Sie dann Details anzeigen aus.
5. Auf der Regelgruppe können Sie Einstellungen anzeigen und bearbeiten.

   Informationen zu den Werten für Regelgruppen finden Sie unter Regelgruppeneinstellungen in der DNS-Firewall.

   Informationen zu den Werten für Regeln finden Sie unter Regeleinstellungen in der DNS-Firewall.

Löschen einer Regelgruppe

Gehen Sie wie folgt vor, um eine Regelgruppe zu löschen.

> **Important**
>
> Wenn Sie eine Regelgruppe löschen, die einer VPC zugeordnet ist, entfernt die DNS-Firewall die Zuordnung und stoppt die Schutzmaßnahmen, die die Regelgruppe für die VPC bereitstellte.

DNS-Firewall-Entitäten löschen

Wenn Sie eine Entität löschen, die Sie in der DNS-Firewall verwenden können, z. B. eine Domainliste, die möglicherweise in einer Regelgruppe verwendet wird, oder eine Regelgruppe, die einer VPC zugeordnet ist, überprüft die DNS-Firewall, ob die Entität derzeit verwendet wird. Wenn es feststellt, dass es verwendet wird, warnt die DNS-Firewall Sie. DNS Firewall kann fast immer bestimmen, ob eine Entität verwendet wird. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die Entität derzeit nicht verwendet, überprüfen Sie sie in Ihren DNS-Firewall-Konfigurationen, bevor Sie sie löschen. Wenn es sich bei der Entität um eine referenzierte Domainliste handelt, stellen Sie sicher, dass keine Regelgruppen sie verwenden. Wenn es sich bei der Entität um eine Regelgruppe handelt, überprüfen Sie, ob sie keiner VPCs Regelgruppe zugeordnet ist.

So löschen Sie eine Regelgruppe

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie mit Schritt 3 fort.

   - ODER -

   Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die Seite .

   die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie die Regelgruppe aus, die Sie löschen möchten, wählen Sie dann Löschen und bestätigen Sie den Löschvorgang.

Domain-Listen von Resolver DNS Firewall

Eine Domainliste ist ein wiederverwendbarer Satz von Domainspezifikationen, die Sie in einer DNS-Firewall-Regel innerhalb einer Regelgruppe verwenden. Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, vergleicht die DNS-Firewall Ihre DNS-Abfragen mit den Domainlisten, die in den Regeln verwendet werden. Wenn es eine Übereinstimmung findet, verarbeitet es die DNS-Abfrage gemäß der Aktion der Übereinstimmungsregel. Weitere Informationen zu Regelgruppen und Regeln finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.

Mit Domainlisten können Sie Ihre expliziten Domainspezifikationen von den Aktionen trennen, die Sie für sie ausführen möchten. Sie können eine einzelne Domainliste in mehreren Regeln verwenden, und alle Aktualisierungen, die Sie an der Domainliste vornehmen, wirken sich automatisch auf alle Regeln aus, die sie verwenden.

Domainlisten lassen sich in zwei Hauptkategorien einteilen:

- Verwaltete Domainlisten, die für Sie AWS erstellt und verwaltet werden.
- Eigene Domainlisten, die Sie erstellen und pflegen.

In diesem Abschnitt werden die Arten von verwalteten Domainlisten beschrieben, die Ihnen zur Verfügung stehen, und bietet Anleitungen zum Erstellen und Verwalten Ihrer eigenen Domainlisten, wenn Sie dies wünschen.

Verwaltete Domainlisten

Verwaltete Domainlisten enthalten Domainnamen, die mit böswilligen Aktivitäten oder anderen potenziellen Bedrohungen in Verbindung stehen. AWS verwaltet diese Listen, damit Route 53 VPC Resolver-Kunden ausgehende DNS-Abfragen kostenlos mit ihnen vergleichen können, wenn sie die DNS-Firewall verwenden.

Sich über die sich ständig ändernde Bedrohungslandschaft auf dem Laufenden zu halten, kann zeitaufwändig und teuer sein. Mit verwalteten Domainlisten können Sie Zeit sparen, wenn Sie die DNS-Firewall implementieren und verwenden. AWS aktualisiert die Listen automatisch, wenn neue Sicherheitslücken und Bedrohungen auftauchen. AWS wird häufig vor der Veröffentlichung über neue Sicherheitslücken informiert, sodass die DNS-Firewall häufig Gegenmaßnahmen für Sie ergreifen kann, bevor eine neue Bedrohung allgemein bekannt wird.

Verwaltete Domainlisten können vor gängigen Internet-Bedrohungen schützen und fügen eine weitere Sicherheitsebene für Ihre Anwendungen hinzu. Die AWS verwalteten Domainlisten beziehen ihre Daten sowohl aus internen AWS Quellen als RecordedFutureauch aus internen Quellen und werden ständig aktualisiert. AWS Verwaltete Domänenlisten sind jedoch nicht als Ersatz für andere Sicherheitskontrollen gedacht Amazon GuardDuty, z. B. solche, die von den ausgewählten AWS Ressourcen bestimmt werden.

Als bewährte Methode sollten Sie eine verwaltete Domainliste in einer Nicht-Produktionsumgebung testen, bevor Sie sie in der Produktion verwenden, wobei die Regelaktion auf `Alert` festgelegt ist. Evaluieren Sie die Regel anhand von CloudWatch Amazon-Metriken in Kombination mit von Resolver

DNS Firewall gesammelten Anfragen oder DNS-Firewall-Protokollen. Wenn Sie überzeugt sind, dass die Regel das tut, was Sie wollen, ändern Sie die Aktionseinstellung nach Bedarf.

Verfügbare AWS verwaltete Domainlisten

In diesem Abschnitt werden die derzeit verfügbaren Listen der verwalteten Domains beschrieben. Wenn Sie sich in einer Region befinden, in der diese Listen unterstützt werden, werden sie in der Konsole angezeigt, wenn Sie Domainlisten verwalten und wenn Sie die Domainliste für eine Regel angeben. In den Protokollen wird die Domainliste innerhalb der `firewall_domain_list_id field` protokolliert.

AWS bietet die folgenden verwalteten Domänenlisten in den Regionen, in denen sie verfügbar sind, für alle Benutzer der Resolver DNS Firewall.

- `AWSManagedDomainsMalwareDomainList` – – Domains, die mit dem Senden von Malware, Hosting von Malware oder dem Verteilen von Malware in Verbindung gebracht werden.
- `AWSManagedDomainsBotnetCommandandControl` – Domains, die mit der Kontrolle von Computernetzwerken verbunden sind, die mit Spam-Malware infiziert sind.
- `AWSManagedDomainsAggregateThreatList`— Domänen, die mehreren DNS-Bedrohungskategorien zugeordnet sind, darunter Malware, Ransomware, Botnet, Spyware und DNS-Tunneling, um verschiedene Arten von Bedrohungen zu blockieren. `AWSManagedDomainsAggregateThreatList`umfasst alle Domänen in den anderen hier AWS aufgelisteten verwalteten Domainlisten.
- `AWSManagedDomainsAmazonGuardDutyThreatList`— Domains, die mit Amazon GuardDuty DNS-Sicherheitsergebnissen verknüpft sind. Die Domains stammen ausschließlich aus den GuardDuty Bedrohungsinformationssystemen von und enthalten keine Domains, die aus externen Quellen Dritter stammen. Insbesondere blockiert diese Liste derzeit nur Domains, die intern generiert und für folgende Erkennungen verwendet wurden: Impact:/.Reputation, Impact GuardDuty:/.Reputation, Impact:EC2/AbusedDomainRequest.Reputation, Impact:EC2/BitcoinDomainRequest.Reputation, Impact: EC2 MaliciousDomainRequest .Reputation. Runtime/AbusedDomainRequest.Reputation, Impact:Runtime/BitcoinDomainRequest.Reputation, and Impact:Runtime/MaliciousDomainRequest

  Weitere Informationen finden Sie im GuardDuty Amazon-Benutzerhandbuch unter Typen suchen.

AWS Verwaltete Domainlisten können nicht heruntergeladen oder durchsucht werden. Um geistiges Eigentum zu schützen, können Sie die einzelnen Domainspezifikationen in AWS verwalteten Domainlisten nicht anzeigen oder bearbeiten. Diese Einschränkung trägt auch dazu bei, böswillige

Benutzer daran zu hindern, Bedrohungen zu entwickeln, die speziell zur Umgehung veröffentlichter Listen dienen.

Um die Listen der verwalteten Domänen zu testen

Zum Testen der verwalteten Domainlisten stehen folgende Domains zur Verfügung:

AWSManagedDomainsBotnetCommandandControl

- controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsMalwareDomainList

- controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsAggregateThreatList und AWSManaged DomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

Diese Domains werden in 1.2.3.4 aufgelöst, wenn sie nicht blockiert werden. Wenn Sie die verwalteten Domainlisten in einer VPC verwenden, wird bei der Abfrage dieser Domains die Antwort zurückgegeben, auf die eine Blockaktion in der Regel festgelegt ist (z. B. NODATA).

Weitere Informationen zu verwalteten Domainlisten erhalten Sie vom AWS Support -Center.

In der folgenden Tabelle sind die verfügbaren Regionen für AWS verwaltete Domainlisten aufgeführt.

Verfügbarkeit verwalteter Domainlisten nach Region

Region	Sind verwaltete Domainlisten verfügbar?
Afrika (Kapstadt)	Ja
Asien-Pazifik (Hongkong)	Ja

Region	Sind verwaltete Domainlisten verfügbar?
Asien-Pazifik (Hyderabad)	Ja
Asien-Pazifik (Jakarta)	Ja
Asien-Pazifik (Malaysia)	Ja
Asien-Pazifik (Melbourne)	Ja
Asien-Pazifik (Mumbai)	Ja
Region Asien-Pazifik (Osaka)	Ja
Asien-Pazifik (Seoul)	Ja
Asien-Pazifik (Singapore)	Ja
Asien-Pazifik (Sydney)	Ja
Asien-Pazifik (Thailand)	Ja
Asien-Pazifik (Tokyo)	Ja
Region Kanada (Zentral)	Ja
Kanada West (Calgary)	Ja
Region Europa (Frankfurt)	Ja

Region	Sind verwaltete Domainlisten verfügbar?
Region Europa (Irland)	Ja
Region Europa (London)	Ja
Europa (Milan)	Ja
Region Europa (Paris)	Ja
Europa (Spain)	Ja
Europa (Stockholm)	Ja
Europa (Zürich)	Ja
Israel (Tel Aviv)	Ja
Middle East (Bahrain)	Ja
Naher Osten (VAE)	Ja
Südamerika (São Paulo)	Ja
USA Ost (Nord-Virginia)	Ja
USA Ost (Ohio)	Ja
USA West (Nordkalifornien)	Ja

Region	Sind verwaltete Domainlisten verfügbar?
USA West (Oregon)	Ja
China (Peking)	Ja
China (Ningxia)	Ja
AWS GovCloud (US)	Ja

Zusätzliche Sicherheitsüberlegungen

AWS Verwaltete Domainlisten sollen Sie vor gängigen Internet-Bedrohungen schützen. Bei Verwendung gemäß der Dokumentation fügen diese Listen eine weitere Sicherheitsebene für Ihre Anwendungen hinzu. Verwaltete Domainlisten sind jedoch nicht als Ersatz für andere Sicherheitskontrollen gedacht, die durch die von Ihnen ausgewählten AWS -Ressourcen bestimmt werden. Wie Sie sicherstellen können, dass Ihre Ressourcen ordnungsgemäß geschützt AWS sind, finden Sie unter Modell der gemeinsamen Verantwortung.

Beseitigung von False-Positive-Szenarien

Wenn Sie in Regeln, die verwaltete Domainlisten zum Blockieren von Abfragen verwenden, auf falsch positive Szenarien stoßen, führen Sie die folgenden Schritte aus:

1. Identifizieren Sie in den VPC-Resolver-Protokollen die Regelgruppe und die Liste der verwalteten Domänen, die den Fehlalarm verursacht haben. Dazu finden Sie das Protokoll für die Abfrage, die die DNS-Firewall blockiert, aber die Sie zulassen möchten. Der Protokolldatensatz listet die Regelgruppe, die Regelaktion und die verwalteten Liste auf. Weitere Informationen über Protokolle finden Sie unter Werte, die in den VPC Resolver-Abfrageprotokollen erscheinen.
2. Erstellen Sie eine neue Regel in der Regelgruppe, die die blockierte Abfrage explizit zulässt. Wenn Sie die Regel erstellen, können Sie Ihre eigene Domainliste nur mit der Domainspezifikation definieren, die Sie zulassen möchten. Folgen Sie den Anweisungen zur Regelgruppen- und Regelverwaltung unter Erstellen einer Regelgruppe und -regeln.

3. Priorisieren Sie die neue Regel innerhalb der Regelgruppe, sodass sie vor der Regel ausgeführt wird, die die verwalteten Liste verwendet. Geben Sie dazu der neuen Regel eine niedrigere numerische Prioritätseinstellung.

Wenn Sie Ihre Regelgruppe aktualisiert haben, lässt die neue Regel explizit den Domainnamen zu, den Sie zulassen möchten, bevor die Blockierungsregel ausgeführt wird.

Verwaltung Ihrer eigenen Domainlisten

Sie können eigene Domainlisten erstellen, um Domainkategorien anzugeben, die Sie entweder nicht in den verwalteten Domainlistenangeboten finden oder die Sie lieber selbst bearbeiten.

Zusätzlich zu den in diesem Abschnitt beschriebenen Verfahren können Sie in der Konsole eine Domänenliste im Kontext der Resolver DNS-Firewall-Regelverwaltung erstellen, wenn Sie eine Regel erstellen oder aktualisieren.

Jede Domainspezifikation in Ihrer Domainliste muss die folgenden Anforderungen erfüllen:

- Es kann optional mit * (Sternchen) beginnen.
- Mit Ausnahme des optionalen Startsterisks und eines Punktes als Trennzeichen zwischen Bezeichnungen darf es nur die folgenden Zeichen enthalten:,`A-Z`, `a-z0-9`, `-` (Bindestrich).
- Es muss 1 bis 255 Zeichen lang sein.

Wenn Sie Änderungen an DNS-Firewall-Entitäten wie Regeln und Domainlisten vornehmen, werden die Änderungen überall dort weitergegeben, wo die Entitäten gespeichert und verwendet werden. Ihre Änderungen werden innerhalb von Sekunden angewendet, es kann jedoch zu einer kurzen Inkonsistenzzeit kommen, wenn die Änderungen an einigen Stellen und nicht an anderen Stellen eingetroffen sind. Wenn Sie beispielsweise eine Domain zu einer Domainliste hinzufügen, auf die durch eine Sperrregel verwiesen wird, wird die neue Domain möglicherweise kurz in einem Bereich Ihrer VPC blockiert, während sie in einem anderen Bereich weiterhin zulässig ist. Diese temporäre Inkonsistenz kann auftreten, wenn Sie die Regelgruppe und VPC-Zuordnungen zum ersten Mal konfigurieren und vorhandene Einstellungen ändern. Im Allgemeinen dauern alle Inkonsistenzen dieses Typs nur wenige Sekunden.

Testen Sie Ihre Domainliste, bevor Sie sie in der Produktion verwenden

Als bewährte Methode sollten Sie eine Domainliste in einer Nicht-Produktionsumgebung testen, bevor Sie sie in der Produktion verwenden, wobei die Regelaktion auf `Alert` festgelegt ist. Evaluieren

Sie die Regel anhand von CloudWatch Amazon-Metriken und den VPC-Resolver-Protokollen. Die Protokolle enthalten den Namen der Domainliste für alle Warnungen und Blockierungsaktionen. Wenn Sie sicher sind, dass die Domainliste Ihren DNS-Abfragen entspricht, wie gewünscht, ändern Sie die Einstellung für die Regelaktion nach Bedarf. Informationen zu CloudWatch Metriken und den Abfrageprotokollen finden Sie unter Überwachung von Resolver-DNS-Firewall-Regelgruppen mit Amazon CloudWatchWerte, die in den VPC Resolver-Abfrageprotokollen erscheinen, und. Konfigurationen für die Protokollierung von Resolver-Abfragen verwalten

So fügen Sie eine Domainliste hinzu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen. Fahren Sie fort mit Schritt 2.

   - ODER -

   Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die Seite .

   die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Domainlisten aus. Auf der Seite Domainlisten können Sie vorhandene Domainlisten auswählen und bearbeiten sowie eigene hinzufügen.
3. Um eine Domainliste hinzuzufügen, wählen Sie Domainliste hinzufügen.
4. Geben Sie einen Namen für Ihre Domainliste ein, und geben Sie dann Ihre Domainspezifikationen in das Textfeld ein (jeweils 1 pro Zeile).

   Wenn Sie Umschalten zum Massen-Upload auf Ein schieben, geben Sie den URI des Amazon-S3-Buckets ein, in dem Sie eine Domainliste erstellt haben. Diese Domainliste sollte einen Domainnamen pro Zeile haben.

   > **Note**
   >
   > Doppelte Domainnamen führen dazu, dass der Massenimport fehlschlägt.
5. Klicken Sie auf Domainliste hinzufügen. Auf der Seite Domainlisten wird Ihre neue Domainliste aufgeführt.

Nachdem Sie die Domainliste erstellt haben, können Sie sie nach Namen aus Ihren DNS-Firewall-Regeln referenzieren.

DNS-Firewall-Entitäten löschen

Wenn Sie eine Entität löschen, die Sie in der DNS-Firewall verwenden können, z. B. eine Domainliste, die möglicherweise in einer Regelgruppe verwendet wird, oder eine Regelgruppe, die einer VPC zugeordnet ist, überprüft die DNS-Firewall, ob die Entität derzeit verwendet wird. Wenn es feststellt, dass es verwendet wird, warnt die DNS-Firewall Sie. DNS Firewall kann fast immer bestimmen, ob eine Entität verwendet wird. In seltenen Fällen ist dies jedoch nicht möglich. Wenn Sie sicherstellen müssen, dass die Entität derzeit nicht verwendet, überprüfen Sie sie in Ihren DNS-Firewall-Konfigurationen, bevor Sie sie löschen. Wenn es sich bei der Entität um eine referenzierte Domainliste handelt, stellen Sie sicher, dass keine Regelgruppen sie verwenden. Wenn es sich bei der Entität um eine Regelgruppe handelt, überprüfen Sie, ob sie keiner Regelgruppe zugeordnet ist VPCs.

So löschen Sie eine Domainliste

1. Wählen Sie im Navigationsbereich Domainlisten aus.
2. Wählen Sie in der Navigationsleiste die Region für die Domainliste aus.
3. Wählen Sie die Domainliste aus, die Sie löschen möchten, wählen Sie dann Löschen und bestätigen Sie den Löschvorgang.

Resolver DNS Firewall Advanced

DNS Firewall Advanced erkennt verdächtige DNS-Abfragen auf der Grundlage bekannter Bedrohungssignaturen in DNS-Abfragen. Sie können einen Bedrohungstyp in einer Regel angeben, die Sie in einer DNS-Firewallregel innerhalb einer Regelgruppe verwenden. Wenn Sie einer VPC eine Regelgruppe zuordnen, vergleicht die DNS-Firewall Ihre DNS-Abfragen mit den Domänen, die in den Regeln gekennzeichnet sind. Wenn es eine Übereinstimmung findet, verarbeitet es die DNS-Abfrage gemäß der Aktion der Übereinstimmungsregel.

DNS Firewall Advanced identifiziert verdächtige DNS-Bedrohungssignaturen, indem es eine Reihe von Schlüsselkennungen in der DNS-Payload untersucht, darunter den Zeitstempel der Anfragen, die Häufigkeit von Anfragen und Antworten, die DNS-Abfragezeichenfolgen sowie die Länge, Art oder Größe sowohl ausgehender als auch eingehender DNS-Abfragen. Je nach Art der Bedrohungssignatur können Sie Richtlinien so konfigurieren, dass die Anfrage blockiert oder einfach protokolliert und eine Warnung angezeigt wird. Durch die Verwendung eines erweiterten Satzes von

Bedrohungskennungen können Sie sich vor DNS-Bedrohungen schützen, die von Domänenquellen stammen, die möglicherweise noch nicht durch Threat-Intelligence-Feeds, die von der breiteren Sicherheitsgemeinschaft verwaltet werden, noch nicht klassifiziert wurden.

Derzeit bietet DNS Firewall Advanced Schutz vor:

- Algorithmen zur Domain-Generierung () DGAs

  DGAs werden von Angreifern verwendet, um eine große Anzahl von Domains zu generieren, um Malware-Angriffe zu starten.
- DNS-Tunneling

  DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.
- Wörterbuch: DGA

  Wörterbücher DGAs werden von Angreifern verwendet, um mithilfe von Wörterbuchwörtern Domains zu generieren, um der Entdeckung in der command-and-control Malware-Kommunikation zu entgehen.

Informationen zum Erstellen von Regeln finden Sie unter Erstellen einer Regelgruppe und -regeln undRegeleinstellungen in der DNS-Firewall.

Beseitigung von False-Positive-Szenarien

Wenn Sie in Regeln, die erweiterte DNS-Firewall-Schutzfunktionen zum Blockieren von Abfragen verwenden, auf falsch positive Szenarien stoßen, gehen Sie wie folgt vor:

1. Identifizieren Sie in den VPC-Resolver-Protokollen die Regelgruppe und die erweiterten Schutzmaßnahmen der DNS-Firewall, die den Fehlalarm verursacht haben. Dazu finden Sie das Protokoll für die Abfrage, die die DNS-Firewall blockiert, aber die Sie zulassen möchten. Im Protokolleintrag sind die Regelgruppe, die Regelaktion und der erweiterte DNS-Firewall-Schutz aufgeführt. Weitere Informationen über Protokolle finden Sie unter Werte, die in den VPC Resolver-Abfrageprotokollen erscheinen.
2. Erstellen Sie eine neue Regel in der Regelgruppe, die die blockierte Abfrage explizit zulässt. Wenn Sie die Regel erstellen, können Sie Ihre eigene Domainliste nur mit der Domainspezifikation definieren, die Sie zulassen möchten. Folgen Sie den Anweisungen zur Regelgruppen- und Regelverwaltung unter Erstellen einer Regelgruppe und -regeln.

3. Priorisieren Sie die neue Regel innerhalb der Regelgruppe, sodass sie vor der Regel ausgeführt wird, die die verwalteten Liste verwendet. Geben Sie dazu der neuen Regel eine niedrigere numerische Prioritätseinstellung.

Wenn Sie Ihre Regelgruppe aktualisiert haben, lässt die neue Regel explizit den Domainnamen zu, den Sie zulassen möchten, bevor die Blockierungsregel ausgeführt wird.

Konfigurieren der Protokollierung für DNS Firewall

Sie können Ihre DNS-Firewall-Regeln anhand von CloudWatch Amazon-Metriken und Resolver-Abfrageprotokollen auswerten. Die Protokolle enthalten den Namen der Domainliste für alle Warnungen und Blockierungsaktionen. Weitere Informationen zu Amazon finden CloudWatch Sie unterÜberwachung von Resolver-DNS-Firewall-Regelgruppen mit Amazon CloudWatch.

Wenn Sie die DNS-Firewall aktivieren, ordnen Sie sie einer VPC zu und Sie haben die Protokollierung aktiviert, `firewall_rule_group_id`, `firewall_rule_action` und `firewall_domain_list_id` sind die DNS-Firewall-spezifischen Felder, die in Ihren Protokollen bereitgestellt werden.

> **Note**
>
> In den Abfrageprotokollen werden die zusätzlichen DNS-Firewall-Felder nur für die Abfragen angezeigt, die durch DNS-Firewall-Regeln blockiert werden.

Um mit der Protokollierung der DNS-Abfragen zu beginnen, die nach DNS-Firewall-Regeln gefiltert werden, die ihren Ursprung in Ihrem haben VPCs, führen Sie die folgenden Aufgaben in der Amazon Route 53-Konsole aus:

So konfigurieren Sie die Protokollierung der Resolver-Abfrage für die DNS-Firewall

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie das Route-53-Konsolenmenü. Wählen Sie oben links in der Konsole die drei horizontalen Balken

   (☰)

   aus.

3. Wählen Sie im Resolver-Menü die Option Abfrageprotokollierung.
4. Wählen Sie in der Regionsauswahl die AWS Region aus, in der Sie die Konfiguration für die Abfrageprotokollierung erstellen möchten.

   Dies muss dieselbe Region sein, in der Sie VPCs die mit der DNS-Firewall verknüpften Regionen erstellt haben, für die Sie Abfragen protokollieren möchten. Wenn Sie VPCs in mehreren Regionen arbeiten, müssen Sie mindestens eine Konfiguration für die Abfrageprotokollierung für jede Region erstellen.
5. Wählen Sie Konfigurieren der Abfrageprotokollierung.
6. Geben Sie die folgenden Werte an:

   Name der Abfrageprotokollierungskonfiguration

   Geben Sie einen Namen für Ihre Abfrageprotokollierungskonfiguration ein. Der Name wird in der Konsole in der Liste der Konfigurationen für die Abfrageprotokollierung angezeigt. Geben Sie einen Namen ein, den Sie später bei der Suche nach dieser Konfiguration unterstützen.

   Ziel der Abfrageprotokolle

   Wählen Sie den AWS Ressourcentyp aus, an den VPC Resolver Abfrageprotokolle senden soll. Informationen zur Auswahl zwischen den Optionen (CloudWatch Logs-Protokollgruppe, S3-Bucket und Firehose-Lieferstream) finden Sie unterAWS Ressourcen, an die Sie VPC Resolver-Abfrageprotokolle senden können.

   Nachdem Sie den Ressourcentyp ausgewählt haben, können Sie entweder eine weitere Ressource dieses Typs erstellen oder eine vorhandene Ressource auswählen, die mit dem aktuellen AWS Konto erstellt wurde.

   > **Note**
   >
   > Sie können nur Ressourcen auswählen, die in der AWS -Region erstellt wurden, die Sie in Schritt 4 ausgewählt haben, der Region, in der Sie die Abfrageprotokollierungskonfiguration erstellen. Wenn Sie eine neue Ressource erstellen, wird diese Ressource in derselben Region erstellt.

VPCs um Abfragen zu protokollieren für

Bei dieser Konfiguration für die Abfrageprotokollierung werden DNS-Abfragen protokolliert, die ihren Ursprung in der VPCs von Ihnen ausgewählten Datei haben. Aktivieren Sie das Kontrollkästchen für jede VPC in der aktuellen Region, für die VPC Resolver Abfragen protokollieren soll, und wählen Sie dann Wählen aus.

> **Note**
>
> Die VPC-Protokollzustellung kann für einen bestimmten Zieltyp nur einmal aktiviert werden. Die Protokolle können nicht an mehrere Ziele desselben Typs übermittelt werden. Beispielsweise können VPC-Protokolle nicht an zwei Amazon-S3-Ziele übermittelt werden.

7. Wählen Sie Konfigurieren der Abfrageprotokollierung.

> **Note**
>
> Sie sollten innerhalb weniger Minuten nach erfolgreicher Erstellung der Konfiguration für die Abfrageprotokollierung DNS-Abfragen von Ressourcen in Ihrer VPC in den Protokollen anzeigen.

Resolver-DNS-Firewall-Regelgruppen zwischen Konten teilen AWS

Sie können DNS-Firewall-Regelgruppen für mehrere AWS Konten gemeinsam nutzen. Um Regelgruppen gemeinsam zu nutzen, verwenden Sie AWS Resource Access Manager (AWS RAM). Die DNS-Firewall-Konsole ist in die AWS RAM Konsole integriert. Weitere Informationen zu AWS RAM finden Sie im Resource Access Manager Manager-Benutzerhandbuch.

Beachten Sie Folgendes:

Gemeinsame Regelgruppen zuordnen mit VPCs

Wenn ein anderes AWS Konto eine Regelgruppe mit Ihrem Konto geteilt hat, können Sie sie Ihrem VPCs Konto zuordnen, genauso wie Sie Regelgruppen zuordnen, die Sie erstellt haben.

Weitere Informationen finden Sie unter Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten.

Löschen oder Aufheben der Freigabe einer freigegebenen Regelgruppe

Wenn Sie eine Regelgruppe gemeinsam mit anderen Konten verwenden und dann entweder die Regelgruppe löschen oder die gemeinsame Nutzung beenden, entfernt die DNS-Firewall alle Verknüpfungen, die die anderen Konten zwischen der Regelgruppe und ihren Konten erstellt haben VPCs.

Maximale Einstellungen für Regelgruppen und -zuordnungen

Gemeinsam genutzte Regelgruppen und ihre Verknüpfungen zu VPCs sind in der Anzahl der Konten enthalten, mit denen die Regelgruppen gemeinsam genutzt werden.

Aktuelle Kontingente für DNS-Firewall finden Sie unter Kontingente auf der Resolver DNS Firewall.

Berechtigungen

Um eine Regelgruppe mit einem anderen AWS Konto zu teilen, benötigen Sie die Berechtigung, die PutFirewallRuleGroupPolicyAktion zu verwenden.

Einschränkungen für das AWS Konto, mit dem eine Regelgruppe geteilt wird

Das Konto, für das eine Regelgruppe freigegeben werden, kann die Regelgruppe nicht ändern oder löschen.

Tagging

Nur das Konto, das eine Regelgruppe erstellt hat, kann Tags zu dieser hinzufügen, löschen oder anzeigen.

Führen Sie die folgenden Schritte aus, um den aktuellen Freigabestatus einer Regelgruppe (einschließlich der Regelgruppe, das die Regelgruppe freigegeben hat, oder des Kontos, für das eine Regelgruppe freigegeben wurde) anzuzeigen und um Regelgruppen für ein anderes Konto freizugeben.

Um den Freigabestatus einzusehen und Regelgruppen für ein anderes AWS Konto freizugeben

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Rule groups (Regelgruppen).

3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regelgruppe erstellt haben.

   Die Spalte Sharing status (Freigabestatus) zeigt den aktuellen Freigabestatus der Regelgruppen, die von dem aktuellen Konto erstellt wurden oder die für das aktuelle Konto freigegeben wurden:

   - Nicht geteilt: Das aktuelle AWS Konto hat die Regelgruppe erstellt, und die Regelgruppe wird nicht mit anderen Konten geteilt.
   - Shared by me (Von mir freigegeben): Das aktuelle Konto hat die Regelgruppe erstellt und für ein oder mehrere Konten freigegeben.
   - Shared with me (Für mich freigegeben): Ein anderes Konto hat die Regelgruppe erstellt und für das aktuelle Konto freigegeben.

4. Wählen Sie den Namen der Regelgruppen, für die Sie Freigabeinformationen anzeigen möchten oder die Sie für ein anderes Konto freigeben möchten.

   Auf der *`rule group name`* Seite Regelgruppe: zeigt der Wert unter Besitzer die ID des Kontos an, mit dem die Regelgruppe erstellt wurde. Dies ist das aktuelle Konto, sofern der Wert unter Sharing Status (Freigabestatus) nicht Shared with me (Für mich freigegeben) lautet. In diesem Fall ist Besitzer das Konto, das die Regelgruppe erstellt und sie mit dem aktuellen Konto geteilt hat.

5. Wählen Sie Share (Freigeben), um zusätzliche Informationen anzuzeigen oder die Regelgruppe für ein anderes Konto freizugeben. Abhängig vom Wert für den Freigabestatus wird eine Seite in der AWS RAM Konsole angezeigt:

   - Not shared (Nicht freigegeben): Die Seite Create resource share (Ressourcenfreigabe erstellen) wird angezeigt. Informationen zum Freigeben der Regelgruppe für ein anderes Konto, eine andere Organisationseinheit oder Organisation erhalten Sie unter dem folgenden Schritt.
   - Shared by me (Von mir freigegeben): Die Seite Shared resources (Freigegebene Ressourcen) zeigt die Regelgruppen und andere Ressourcen, die zu dem aktuellen Konto gehören und für andere Konten freigegeben wurden.
   - Shared with me (Für mich freigegeben): Die Seite Shared resources (Freigegebene Ressourcen) zeigt die Regelgruppen und andere Ressourcen, die zu anderen Konten gehören und für das aktuelle Konto freigegeben wurden.

6. Um eine Regelgruppe mit einem anderen AWS Konto, einer anderen Organisationseinheit oder Organisation zu teilen, geben Sie die folgenden Werte an.

> **Note**
>
> Sie können keine Freigabeeinstellungen aktualisieren. Um eine der folgenden Einstellungen zu ändern, müssen Sie eine Regelgruppe mit den neuen Einstellungen freigeben und die alten Freigabeeinstellungen anschließend entfernen.

Description

Geben Sie eine Kurzbeschreibung ein, mit der Sie sich den Grund für die Freigabe der Regelgruppe merken können.

Ressourcen

Aktivieren Sie das Kontrollkästchen für die Regelgruppe, die Sie freigeben möchten.

Prinzipale

Geben Sie die AWS Kontonummer, den Namen der Organisationseinheit oder den Namen der Organisation ein.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können beispielsweise Cost center für Key und 456 für Value angeben.

Dies sind die Tags, mit AWS Fakturierung und Kostenmanagement denen Sie Ihre AWS Rechnung organisieren können. Sie können Tags auch für andere Zwecke verwenden. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

Aktivierung des Resolver-DNS-Firewall-Schutzes für Ihre VPC

Sie aktivieren den Schutz der DNS-Firewall für Ihre VPC, indem Sie einer oder mehreren Regelgruppen der VPC zuordnen. Immer wenn eine VPC einer DNS-Firewall-Regelgruppe zugeordnet ist, bietet Route 53 VPC Resolver die folgenden DNS-Firewall-Schutzmaßnahmen:

- VPC Resolver leitet die ausgehenden DNS-Abfragen der VPC über die DNS-Firewall weiter, und die DNS-Firewall filtert die Abfragen mithilfe der zugehörigen Regelgruppen.
- VPC Resolver erzwingt die Einstellungen in der DNS-Firewall-Konfiguration der VPC.

Um DNS-Firewall-Schutz für Ihre VPC bereitzustellen, gehen Sie wie folgt vor:

- Erstellen und verwalten Sie Verknüpfungen zwischen Ihren DNS-Firewall-Regelgruppen und Ihrer VPC. Informationen zu Regelgruppen finden Sie unter DNS-Firewall-Regelgruppen und -Regeln.
- Konfigurieren Sie, wie VPC Resolver DNS-Abfragen für die VPC während eines Fehlers verarbeiten soll, z. B. wenn die DNS-Firewall keine Antwort auf eine DNS-Anfrage liefert.

Zuordnungen zwischen Ihrer VPC und der Resolver DNS Firewall-Regelgruppe verwalten

So zeigen Sie die VPC Zuordnungen einer Regelgruppe an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/

   Wählen Sie im Navigationsbereich die Option DNS-Firewall aus, um die Seite Regelgruppen der DNS-Firewall in der Amazon-VPC-Konsole zu öffnen.

   - ODER -

   Melden Sie sich in der AWS-Managementkonsole an und öffnen Sie die Seite .

   die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter DNS-Firewall die Option Regelgruppen aus.
3. Wählen Sie in der Navigationsleiste die Region für die Regelgruppe aus.
4. Wählen Sie die Regelgruppe aus, die Sie zuordnen möchten.
5. Wählen Sie die Option Details anzeigen aus. Die Regelgruppe wird angezeigt.
6. Unten sehen Sie einen Detailbereich mit Registern, der Regeln und zugehörige Regeln enthält. VPCs Wählen Sie die Registerkarte Zugeordnet. VPCs

So verknüpfen Sie eine Regelgruppe mit einer VPC

1. Suchen Sie die VPC-Zuordnungen der Regelgruppe, indem Sie die Anweisungen im vorherigen Verfahren So zeigen Sie die VPC-Zuordnungen einer Regelgruppe befolgen.
2. Wählen Sie auf der VPCs Registerkarte Zugeordnet die Option Associate VPC aus.

3. Suchen Sie im Dropdown-Menü die VPC, die Sie mit der Regelgruppe verknüpfen möchten. Wählen Sie es aus und wählen Sie Zuordnung von aus.

Auf der Regelgruppenseite ist Ihre VPC auf der VPCs Registerkarte Zugeordnet aufgeführt. Zunächst meldet der Status der Zuordnung Aktualisieren. Wenn die Zuordnung abgeschlossen ist, ändert sich der Status in Abgeschlossen.

So entfernen Sie eine Zuordnung zwischen einer Regelgruppe und einer VPC

1. Suchen Sie die VPC-Zuordnungen der Regelgruppe, indem Sie die Anweisungen im vorherigen Verfahren So zeigen Sie die VPC-Zuordnungen einer Regelgruppe befolgen.
2. Wählen Sie die VPC aus, die Sie aus der Liste entfernen möchten, und wählen Sie dann Disassociate aus. Überprüfen Sie und bestätigen Sie die Aktion.

Auf der Regelgruppenseite wird Ihre VPC auf der VPCs Registerkarte Zugeordnet mit dem Status Disassociated aufgeführt. Nach Abschluss des Vorgangs aktualisiert die DNS-Firewall die Liste, um die VPC zu entfernen.

Konfiguration der DNS-Firewall-VPC

Die DNS-Firewall-Konfiguration für Ihre VPC bestimmt, ob Route 53 VPC Resolver Abfragen zulässt oder sie bei Ausfällen blockiert, z. B. wenn die DNS-Firewall beeinträchtigt ist, nicht reagiert oder in der Zone nicht verfügbar ist. VPC Resolver erzwingt die Firewallkonfiguration einer VPC, wenn Sie eine oder mehrere DNS-Firewall-Regelgruppen mit der VPC verknüpft haben.

Sie können eine VPC so konfigurieren, dass sie nicht geöffnet oder nicht geschlossen wird.

- Standardmäßig ist der Fehlermodus geschlossen, was bedeutet, dass VPC Resolver alle Abfragen blockiert, für die er keine Antwort von der DNS-Firewall erhält, und eine `SERVFAIL` DNS-Antwort sendet. Dieser Ansatz begünstigt Sicherheit gegenüber Verfügbarkeit.
- Wenn Sie Fail Open aktivieren, lässt VPC Resolver Abfragen durch, wenn er keine Antwort von der DNS-Firewall erhält. Dieser Ansatz begünstigt die Verfügbarkeit gegenüber der Sicherheit.

So ändern Sie die Konfiguration der DNS-Firewall für eine VPC (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die VPC Resolver-Konsole unter. https://console.aws.amazon.com/route53resolver/

2. Wählen Sie im Navigationsbereich unter Resolvers die Option. VPCs
3. Suchen und bearbeiten Sie auf der VPCsSeite die VPC. Ändern Sie die Konfiguration der DNS-Firewall so, dass sie bei Bedarf nicht geöffnet oder nicht geschlossen wird.

So ändern Sie das Verhalten der DNS-Firewall für eine VPC (API)

- Aktualisieren Sie Ihre VPC-Firewallkonfiguration, indem Sie anrufen UpdateFirewallConfigund diese aktivieren oder deaktivieren `FirewallFailOpen`.

Sie können eine Liste Ihrer VPC-Firewall-Konfigurationen über die API abrufen, indem Sie aufrufen ListFirewallConfigs.

Was sind Amazon Route 53 53-Profile?

Mit Route 53 53-Profilen können Sie DNS-bezogene Route 53-Konfigurationen auf viele VPCs und unterschiedliche Arten anwenden und verwalten. AWS-Konten Profile machen die Verwaltung der DNS-Einstellungen für viele VPCs so einfach wie die Verwaltung für eine einzelne VPC. Wenn Sie ein Profil aktualisieren, werden seine Einstellungen an alle VPCs mit dem Profil verknüpften Personen weitergegeben. Sie können ein Profil auch mit denselben AWS-Konten Regionen teilen, indem Sie. AWS RAM Die derzeit von Route 53 unterstützten Ressourcen, die Sie einem Profil zuordnen können, sind:

- Private gehostete Zonen und die darin angegebenen Einstellungen. Weitere Informationen zum Arbeiten mit privaten gehosteten Zonen finden Sie unterArbeiten mit privat gehosteten Zonen.
- Resolver-Regeln, sowohl für die Weiterleitung als auch für das System. Weitere Informationen zu Resolver-Regeln finden Sie unter. Verwalten von Weiterleitungsregeln
- DNS-Firewall-Regelgruppen. Weitere Informationen zu DNS-Firewall-Regelgruppen finden Sie unterDNS-Firewall-Regelgruppen und -Regeln.
- Schnittstelle für VPC-Endpunkte. Weitere Informationen zu Schnittstellen-VPC-Endpunkten finden Sie unter Schnittstellen-VPC-Endpunkte im Amazon VPC-Benutzerhandbuch.
- Konfigurationen für die VPC Resolver-Abfrageprotokollierung. Weitere Informationen zur VPC Resolver-Abfrageprotokollierung finden Sie unter. Abfrageprotokollierung

Einige der VPC-Konfigurationen werden direkt im Profil verwaltet. Die Konfigurationen sind:

- Konfiguration der umgekehrten DNS-Suche für Resolver-Regeln.
- Konfiguration des DNS-Firewall-Fehlermodus.
- Konfiguration der DNSSEC-Validierung.

Sie können beispielsweise die Konfiguration des DNS-Firewall-Fehlermodus für alle Dateien aktivieren, denen VPCs das Profil zugeordnet ist, aber die bestehende DNSSEC-Validierungskonfiguration der VPC beibehalten.

> **Important**
>
> Sobald Sie die Profileinstellungen für die vorherigen Konfigurationen aktiviert und das Profil einer VPC zugeordnet haben, werden die Profileinstellungen sofort wirksam.

Sie können sie auch verwenden CloudFormation , um konsistente DNS-Einstellungen für neu bereitgestellte VPCs Dateien einzurichten.

Sie können ein Profil pro VPC zuordnen, und die Anzahl der Ressourcen, die Sie pro Profil zuordnen können, variiert. Weitere Informationen finden Sie unter Kontingente für Route 53 53-Profile .

So werden Route 53 53-Profileinstellungen priorisiert

Sie können die lokalen DNS-Einstellungen und Zuordnungen für Profile für Migrations- oder andere Testzwecke festlegen. Wenn eine DNS-Abfrage sowohl mit der Resolver-Regel für eine private gehostete Zone, die direkt mit der VPC verknüpft ist, als auch mit einer Resolver-Regel für eine private gehostete Zone, die dem Profil zugeordnet ist, übereinstimmt, haben die lokalen DNS-Einstellungen Vorrang. Wenn eine DNS-Abfrage für einen Domainnamen gestellt wird, der in Konflikt steht, gewinnt der spezifischste. Die folgende Tabelle enthält Beispiele für die Reihenfolge der Bewertungen:

DNS-Abfrage	Profilregel	VPC-Regel	Evaluierte Regel
example.com	example.com	example.com	Lokale VPC
test.example.com	test.example.com	example.com	Profil
marketing.example.com	Keine	marketing.example.com	Lokale VPC

Route 53 53-Profile — Verfügbarkeit in der Region

Informationen zur Verfügbarkeit in der Region und zu den Endpunkten finden Sie unter Service-Endpunkte für Route 53 im AWS Allgemeinen Referenzhandbuch.

Allgemeine Schritte zur Verwendung von Route 53 53-Profilen

Um Amazon Route 53 53-Profile in Ihrer Amazon Virtual Private Cloud zu implementieren VPCs, führen Sie die folgenden allgemeinen Schritte aus.

1. Erstellen Sie ein leeres Profil — Der erste Schritt besteht darin, ein leeres Profil zu erstellen, dem Sie DNS-Ressourcen zuordnen können. Weitere Informationen finden Sie unter Route 53 53-Profile erstellen.
2. DNS-Ressourcen dem Profil zuordnen — Bei den Ressourcen, die Sie derzeit einem Profil zuordnen können, handelt es sich um private gehostete Zonen, Resolver-Regeln (sowohl für Weiterleitung als auch für System), DNS-Firewall-Regelgruppen, VPC-Resolver-Abfrageprotokollierungskonfigurationen und VPC-Schnittstellen-Endpunkte. Weitere Informationen dazu finden Sie unter Zuordnen von DNS-Firewall-Regelgruppen zu einem Route-53-Profil, Zuordnen von privaten gehosteten Zonen zu einem Route-53-Profil, Zuordnen von Resolver-Regeln zu einem Route-53-Profil, Ordnen Sie die Konfigurationen der VPC Resolver-Abfrageprotokollierung einem Route 53 53-Profil zu und Schnittstellen-VPC-Endpunkte einem Route 53 53-Profil zuordnen.
3. Konfigurieren Sie einige der VPC-Einstellungen für das Profil — Einige der DNS-Einstellungen, z. B. gehostete Zonen, die dem Profil zugeordnet sind, werden VPCs sofort auf das angewendet. Für die Konfiguration von DNSSEC-Validierung, Resolver, Reverse-DNS-Suche und DNS-Firewall-Fehlermodus können Sie eine der folgenden Optionen wählen:
   - Für die DNSSEC-Validierung können Sie wählen, ob Sie die lokale VPC-Konfiguration (Standard) verwenden, die Validierung aktivieren oder die Validierung für alle mit dem Profil VPCs verknüpften Objekte deaktivieren möchten.
   - Für die Reverse-DNS-Suchkonfiguration von Resolver können Sie sie aktivieren, deaktivieren oder die auto definierten Regeln verwenden, die lokal für die VPC definiert sind (Standard).
   - Für die Konfiguration des DNS-Firewall-Fehlermodus können Sie ihn aktivieren, deaktivieren oder die für die VPC lokal definierte Fehlermoduskonfiguration verwenden (Standard).

   Weitere Informationen finden Sie unter Route 53 53-Profilkonfigurationen bearbeiten.
4. Ordnen Sie das Profil einem oder mehreren zu VPCs — Um Ihr Profil verwenden zu können, ordnen Sie es einem oder mehreren VPCs zu. Weitere Informationen finden Sie unter Ordnen Sie ein Route 53 53-Profil zu VPCs.

Route 53 53-Profile erstellen

Folgen Sie den Anweisungen in diesem Thema, um Route 53 53-Profile zu erstellen. Wählen Sie eine Registerkarte, um mithilfe der Route 53 53-Konsole ein Route 53-Profil zu erstellen, oder AWS CLI.

- Konsole
- CLI

Console

So erstellen Sie ein Route 53 53-Profil

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellen möchten.
4. Geben Sie einen Namen für das Profil ein, fügen Sie optional Tags hinzu und wählen Sie Profil erstellen.

   Dadurch wird ein leeres Profil mit Standardkonfigurationen erstellt, denen Sie Ressourcen zuordnen können. Nachdem Sie dem Profil Ressourcen zugeordnet haben, können Sie es einer Reihe von Objekten zuordnen VPCs und bearbeiten, wie einige der Resolver-Konfigurationen auf das VPCs angewendet werden.

CLI

Sie können ein Profil erstellen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für `name` verwenden.

```
aws route53profiles create-profile --name test
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
```

```
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```


Gehen Sie wie folgt vor, um Ihre Profile verschiedenen Ressourcen zuzuordnen und die VPC-Konfigurationen für das Profil zu bearbeiten:

Themen

- Zuordnen von DNS-Firewall-Regelgruppen zu einem Route-53-Profil
- Zuordnen von privaten gehosteten Zonen zu einem Route-53-Profil
- Zuordnen von Resolver-Regeln zu einem Route-53-Profil
- Schnittstellen-VPC-Endpunkte einem Route 53 53-Profil zuordnen
- Ordnen Sie die Konfigurationen der VPC Resolver-Abfrageprotokollierung einem Route 53 53-Profil zu
- Route 53 53-Profilkonfigurationen bearbeiten
- Ordnen Sie ein Route 53 53-Profil zu VPCs

Zuordnen von DNS-Firewall-Regelgruppen zu einem Route-53-Profil

Anweisungen zum Erstellen einer Regelgruppe finden Sie unter. Wählen Sie dann eine Registerkarte ausErstellen einer Regelgruppe und -regeln, um mithilfe der Route 53-Konsole DNS-Firewall-Regelgruppen einem Route 53-Profil zuzuordnen, oder AWS CLI.

- Konsole
- CLI

Console

So ordnen Sie DNS-Firewall-Regelgruppen zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. Wählen Sie im Navigationsbereich Profile aus und wählen Sie in der Tabelle Profile den verknüpften Namen des Profils aus, mit dem Sie arbeiten möchten.
4. <Profile name>Wählen Sie auf der Seite die Registerkarte DNS-Firewall-Regelgruppen und dann Zuordnen aus.
5. Im Abschnitt DNS-Firewall-Regelgruppen können Sie bis zu 10 Regelgruppen auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als 10 Regelgruppen zuordnen möchten, verwenden Sie die APIs. Weitere Informationen finden Sie unter AssociateResourceToProfile.

   Informationen zum Erstellen neuer Regelgruppen finden Sie unterErstellen einer Regelgruppe und -regeln.
6. Wählen Sie Weiter aus.
7. Auf der Seite Priorität definieren können Sie die Reihenfolge festlegen, in der die Regelgruppen verarbeitet werden, indem Sie auf die vorab zugewiesene Prioritätsnummer klicken und eine neue eingeben. Die zulässigen Werte für die Priorität liegen zwischen 100 und 9900.

   Die Regelgruppen werden von der niedrigsten numerischen Prioritätseinstellung bis zur höchsten Priorität ausgewertet. Sie können die Priorität einer Regelgruppe jederzeit ändern, um beispielsweise die Reihenfolge der Verarbeitung zu ändern oder Platz für andere Regelgruppen zu schaffen.

   Wählen Sie Absenden aus.
8. Der Status der Zuordnung wird im Dialogfeld DNS-Firewall-Regelgruppen in der Spalte Status angezeigt.

CLI

Sie können eine Regelgruppe einem Profil zuordnen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihre eigenen Werte für `name` `profile-idresource-arn`, und verwenden`priority`:

```
aws route53profiles associate-resource-to-profile --name test-
resource-association --profile-id rp-4987774726example --resource-arn
arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/
rslvr-frg-cfe7f72example --resource-properties "{\"priority\": 102}"
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

Zuordnen von privaten gehosteten Zonen zu einem Route-53-Profil

Anweisungen zum Erstellen einer privaten gehosteten Zone finden Sie unter. Folgen Sie dann den Schritten in diesem VerfahrenErstellen einer privat gehosteten Zone, um eine private gehostete Zone einem Profil zuzuordnen.

So ordnen Sie private Hosting-Zonen zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. Wählen Sie im Navigationsbereich Profile aus und wählen Sie in der Tabelle Profile den verknüpften Namen des Profils aus, mit dem Sie arbeiten möchten.

4. <Profile name>Wählen Sie auf der Seite die Registerkarte Private gehostete Zonen und dann Zuordnen aus.
5. Auf der Seite Private gehostete Zonen zuordnen können Sie bis zu 10 privat gehostete Zonen auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als 10 privat gehostete Zonen zuordnen möchten, verwenden Sie die APIs. Weitere Informationen finden Sie unter AssociateResourceToProfile.

   Informationen zum Erstellen von privaten Hosting-Zonen finden Sie unterErstellen einer privat gehosteten Zone.
6. Wählen Sie Associate
7. Der Zuordnungsfortschritt wird in der Spalte Status auf der Registerkarte Private gehostete Zonen angezeigt.

Zuordnen von Resolver-Regeln zu einem Route-53-Profil

Anweisungen zum Erstellen einer Resolver-Regel finden Sie unter. Folgen Sie anschließend den Schritten in diesem VerfahrenErstellen von Weiterleitungsregeln, um Resolver-Regeln einem Profil zuzuordnen.

So ordnen Sie VPC-Resolver-Regeln zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. <Profile name>Wählen Sie auf der Seite die Registerkarte Resolver-Regeln und dann Zuordnen aus.
4. Auf der Seite „Resolver-Regeln zuordnen“ können Sie in der Tabelle Resolver-Regeln bis zu 10 Resolver-Regeln auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als 10 Resolver-Regeln zuordnen möchten, verwenden Sie die. APIs Weitere Informationen finden Sie unter AssociateResourceToProfile.

   Informationen zum Erstellen von Resolver-Regeln finden Sie unter. Erstellen von Weiterleitungsregeln
5. Wählen Sie Associate
6. Der Zuordnungsfortschritt wird in der Spalte Status auf der Registerkarte Resolver-Regeln angezeigt.

Schnittstellen-VPC-Endpunkte einem Route 53 53-Profil zuordnen

Anweisungen zum Erstellen eines VPC-Schnittstellen-Endpunkts finden Sie unter Erstellen eines VPC-Endpunkts im VPC-Benutzerhandbuch. und folgen Sie dann den Schritten in diesem Verfahren, um einen VPC-Endpunkt einem Profil zuzuordnen.

So ordnen Sie VPC-Endpunkte zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. <Profile name>Wählen Sie auf der Seite die Registerkarte VPC-Endpoints und dann Associate aus.
4. Auf der Seite VPC-Endpoints zuordnen können Sie in der Tabelle VPC-Endpoints bis zu 10 Endpoints auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als 10 Endpunkte zuordnen möchten, verwenden Sie die. APIs Weitere Informationen finden Sie unter AssociateResourceToProfile.

   Informationen zum Erstellen von Resolver-Regeln finden Sie unter. Erstellen von Weiterleitungsregeln
5. Wählen Sie Associate
6. Der Zuordnungsfortschritt wird in der Spalte Status auf der Registerkarte VPC-Endpunkte angezeigt.

Ordnen Sie die Konfigurationen der VPC Resolver-Abfrageprotokollierung einem Route 53 53-Profil zu

Anweisungen zum Erstellen einer VPC-Resolver-Abfrageprotokollierungskonfiguration finden Sie unter. Wählen Sie dann eine Registerkarte ausKonfiguration (VPC Resolver-Abfrageprotokollierung), um die VPC-Resolver-Konfiguration mithilfe der Route 53 53-Konsole einem Route 53-Profil zuzuordnen, oder. AWS CLI

- Konsole
- CLI

Console

So ordnen Sie Konfigurationen für die Abfrageprotokollierung zu

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. Wählen Sie auf der Seite mit dem Profilnamen die Registerkarte Resolver Query Log Configurations und dann Associate aus.
4. Auf der Seite Abfrageprotokollierungskonfigurationen zuordnen können Sie in der Tabelle Resolver-Abfrageprotokollkonfigurationen bis zu drei Konfigurationen auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als drei Konfigurationen für die Abfrageprotokollierung zuordnen möchten, verwenden Sie die API. Weitere Informationen finden Sie unter AssociateResourceToProfile.
5. Informationen zum Erstellen neuer Konfigurationen für die VPC Resolver-Abfrageprotokollierung finden Sie unter. Konfiguration (VPC Resolver-Abfrageprotokollierung)
6. Wählen Sie Associate
7. Der Status der Zuordnung wird auf der Registerkarte Resolver-Abfrageprotokollkonfigurationen in der Spalte Status angezeigt.

CLI

Sie können eine Abfrageprotokollkonfiguration einem Profil zuordnen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihre eigenen Werte für `name` `profile-id` und `resource-arn` verwenden.

```
aws route53profiles associate-resource-to-profile --name test-resource-association --profile-id rp-4987774726example --resource-arn arn:aws:route53resolver:us-east-1:123456789012:resolver-query-log-config/rqlc-cfe7f72example
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851226.613,
        "Id": "rpr-001913120b8example",
```

```
        "ModificationTime": 1710851226.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:resolver-
query-log-config/rqlc-cfe7f72example",
        "ResourceType": "RESOLVER_QUERY_LOG_CONFIG",
        "Status": "CREATING",
        "StatusMessage": "Creating rp-4987774726example to rqlc-cfe7f72example
 association"
    }
}
```

Route 53 53-Profilkonfigurationen bearbeiten

Nachdem Sie Ressourcen einem Profil zugeordnet haben, können Sie die VPC-Standardkonfigurationen bearbeiten, um zu entscheiden, wie sie auf die VPCs angewendet werden.

Um Profilkonfigurationen zu bearbeiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. Wählen Sie im Navigationsbereich Profile aus und wählen Sie in der Tabelle Profile den verknüpften Namen des Profils aus, mit dem Sie arbeiten möchten.
4. <Profile name>Wählen Sie auf der Seite die Registerkarte Konfiguration und dann Bearbeiten aus.
5. Wählen Sie auf der Seite Konfiguration bearbeiten einen der Werte für die VPC-DNSSEC-Konfiguration, die Resolver-Reverse-DNS-Suchkonfiguration und die Konfiguration des DNS-Firewall-Fehlermodus aus.

   Weitere Informationen zu den Werten finden Sie unter. Konfigurationseinstellungen für das Route 53 53-Profil
6. Wählen Sie Aktualisieren aus.

Konfigurationseinstellungen für das Route 53 53-Profil

Wenn Sie eine Route 53 53-Profilkonfiguration bearbeiten, geben Sie die folgenden Werte an:

DNSSEC-Konfiguration

Wählen Sie einen der folgenden Werte aus:

- Lokale VPC-DNSSEC-Konfiguration verwenden — Standard

  Wählen Sie diese Option, damit alle mit diesem Profil VPCs verknüpften Benutzer ihre lokale DNSSEC-Validierungskonfiguration beibehalten.

- DNSSEC-Validierung aktivieren

  Wählen Sie diese Option, um die DNSSEC-Validierung in allen mit diesem Profil VPCs verknüpften Objekten zu aktivieren.

- Deaktivieren Sie die DNSSEC-Validierung

  Wählen Sie diese Option, um die DNSSEC-Validierung in allenVPCs , die diesem Profil zugeordnet sind, zu deaktivieren.

Konfiguration für die umgekehrte DNS-Suche des Resolvers

Wählen Sie einen der folgenden Werte aus:

- Aktivieren

  Wählen Sie diese Option, um auto definierte Regeln für die umgekehrte DNS-Suche in allen zugehörigen Dateien zu erstellen VPCs.

- Nicht aktiviert

  Wählen Sie diese Option, um keine auto definierten Regeln für die umgekehrte DNS-Suche in allen zugehörigen Dateien zu erstellen VPCs.

- Lokale auto definierte Regeln verwenden — Standard

  Wählen Sie diese Option, um die lokalen VPC-Einstellungen für die umgekehrte DNS-Suche für das zugehörige VPCs Objekt zu verwenden.

Konfiguration des DNS-Firewall-Fehlermodus

Wählen Sie einen der folgenden Werte aus:

- Deaktivieren

  Wählen Sie diese Option, um den DNS-Firewall-Fehlermodus für die zugehörige Datei zu schließen VPCs. Mit dieser Option blockiert die DNS-Firewall alle Abfragen, die sie nicht richtig auswerten kann.

- Aktiviert

  Wählen Sie diese Option, um den DNS-Firewall-Fehlermodus für alle zugehörigen Benutzer geöffnet zu lassen VPCs. Mit dieser Option ermöglicht die DNS-Firewall die Fortsetzung von Abfragen, wenn sie nicht ordnungsgemäß ausgewertet werden können.

- Verwenden Sie die Einstellungen für den lokalen Fehlermodus — Standard

  Wählen Sie diese Option, um die lokalen VPC-DNS-Firewall-Fehlermoduseinstellungen zu verwenden.

Weitere Informationen zu den Konfigurationen finden Sie unter

- Aktivieren der DNSSEC-Validierung in Amazon Route 53
- Weiterleitungsregeln für Reverse-DNS-Abfragen in VPC Resolver
- Konfiguration der DNS-Firewall-VPC

Ordnen Sie ein Route 53 53-Profil zu VPCs

Folgen Sie den Anweisungen in diesem Thema, um einer VPC ein Route 53 53-Profil zuzuordnen. Wählen Sie eine Registerkarte, um mithilfe der Route 53 53-Konsole ein Route 53-Profil einer VPC zuzuordnen, oder AWS CLI.

- Konsole
- CLI

Console

Um eine Verbindung herzustellen VPCs

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
3. <Profile name>Wählen Sie auf der Seite die VPCsRegisterkarte und dann Zuordnen aus.
4. Auf der VPCs Seite „Zuordnen“ können Sie bis zu 10 auswählen, die VPCs Sie zuvor erstellt haben. Wenn Sie mehr als 10 verknüpfen möchten VPCs, verwenden Sie die APIs. Weitere Informationen finden Sie unter AssociateProfile.

5. Wählen Sie Assoziieren
6. Der Zuordnungsfortschritt wird in der Spalte Status auf der VPCsSeite angezeigt.

CLI

Sie können die Profile auflisten, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihre eigenen Werte für `nameprofile-id`, und verwenden`resource-id`:

```
aws route53profiles associate-profile --name test-association --profile-
id rp-4987774726example --resource-id vpc-0af3b96b3example
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

Amazon Route 53 53-Profile anzeigen und aktualisieren

Wählen Sie die Registerkarte Konsole, um das Route 53 53-Profil anzuzeigen und zu bearbeiten. Wählen Sie die Registerkarte CLI aus, AWS CLI um Profile aufzulisten, die Ihnen gehören, von Ihnen geteilt oder für Sie freigegeben wurden.

- Konsole
- CLI

Console

Route 53 53-Profile anzeigen und aktualisieren

1. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, das Sie anzeigen oder bearbeiten möchten.
4. Auf der <Profile name>Seite können Sie die aktuell verknüpften DNS-Ressourcen anzeigen, neue zuordnen und die Tags und VPC-Konfigurationen bearbeiten.

CLI

Sie können die Profile auflisten, indem Sie einen AWS CLI Befehl wie den folgenden ausführen:

```
aws route53profiles list-profiles
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

Sie können Informationen über einen bestimmten VPS abrufen, dem das Profil zugeordnet ist, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für `profile-association-id` verwenden:

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Im Folgenden finden Sie eine Beispielausgabe, nachdem Sie den Befehl ausgeführt haben:

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Löschen eines Amazon Route 53 53-Profils

Wählen Sie eine Registerkarte, um ein Route 53 53-Profil mithilfe der Route 53-Konsole zu löschen, oder AWS CLI.

- Konsole
- CLI

Console

So löschen Sie ein Route 53 53-Profil

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, das Sie löschen möchten, und wählen Sie dann Löschen aus.

> **Important**
>
> Sie können ein Profil nicht löschen, wenn es verknüpft ist VPCs. Wenn das Profil mit einem anderen geteilt wird AWS-Konto, gehen außerdem alle VPCs Konfigurationen verloren, mit denen die Profilkonfigurationen verknüpft sind.

4. <Profile name>Geben Sie im Dialogfeld Löschen den Text ein**confirm**, und wählen Sie dann Löschen aus.

CLI

> **Important**
>
> Sie können ein Profil nicht löschen, wenn es verknüpft ist mit VPCs. Wenn das Profil mit einem anderen geteilt wird AWS-Konto, gehen außerdem alle VPCs Konfigurationen verloren, mit denen die Profilkonfigurationen verknüpft sind.

Sie können ein Profil löschen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für verwenden`profile-id`:

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "DELETED",
        "StatusMessage": "Deleted Profile"
    }
}
```

Route 53-Ressourcen, die einem Amazon Route 53-Profil zugeordnet sind, anzeigen und aktualisieren

Wählen Sie die Registerkarte Konsole, um die Ressourcenzuordnungen für das Route 53 53-Profil anzuzeigen, und bearbeiten Sie optional die Priorität der DNS-Firewall-Regelgruppe. Wählen Sie die Registerkarte CLI aus AWS CLI , um die Ressourcenzuordnungen aufzulisten und ein Beispielupdate für eine Priorität einer DNS-Firewall-Regelgruppe anzuzeigen.

- Konsole
- CLI

Console

Um Ressourcen anzuzeigen und zu aktualisieren, die einem Profil zugeordnet sind

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
4. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, für das Sie die Ressourcenzuordnungen anzeigen oder bearbeiten möchten.
5. <Profile name>Wählen Sie auf der Seite die Registerkarte für die Ressource aus, die Sie anzeigen oder bearbeiten möchten, entweder DNS-Firewall-Regelgruppen, Private gehostete Zonen, Resolver-Regeln oder VPC-Endpunkte.
6. Auf der Registerkarte für eine Ressource können Sie die Namen, den ARN und den Status der zugehörigen Ressourcen einsehen. Sie können auch das Zahnradsymbol wählen, um anzupassen, was in der Ressourcentabelle angezeigt wird.

   Auf der Registerkarte DNS-Firewall-Regelgruppen können Sie auch den Prioritätseintrag für die Regelgruppe auswählen und ihn auf eine kleinere oder größere Zahl ändern. Die Regelgruppen werden in der Reihenfolge ausgewertet, angefangen von der niedrigsten Prioritätsnummer bis zur höchsten Prioritätsnummer.

CLI

Sie können einem Profil zugeordnete Ressourcen auflisten, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für verwendenprofile-id:

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileResourceAssociations": [
        {
            "CreationTime": 1710851216.613,
            "Id": "rpr-001913120a7example",
            "ModificationTime": 1710851216.613,
            "Name": "test-resource-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
            "ResourceProperties": "{\"priority\":102}",
            "ResourceType": "FIREWALL_RULE_GROUP",
            "Status": "COMPLETE",
            "StatusMessage": "Completed creation of Profile to DNS Firewall rule
 group association"
        }
    ]
}
```

Sie können die Priorität einer DNS-Firewall-Regelgruppe aktualisieren, die einem Profil zugeordnet ist, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert und Ihre eigenen Werte für profile-resource-association-id und verwenden--resource-properties:

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

Im Folgenden finden Sie eine Beispielausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
```

```
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

Aufheben der Zuordnung einer Ressource zu einem Amazon Route 53 53-Profil

Bevor Sie ein Profil löschen, müssen Sie alle Ressourcen davon trennen.

So trennen Sie die Zuordnung einer Ressource, die einem Route 53 53-Profil zugeordnet ist

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der das Profil erstellt wurde, zu dem Sie die Zuordnung einer Ressource aufheben möchten.
4. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, zu dem Sie die Zuordnung einer Ressource aufheben möchten.
5. Wählen Sie auf der Seite Profilname die Registerkarte für die Ressource aus, die Sie löschen möchten, entweder DNS-Firewall-Regelgruppen, Private gehostete Zonen, Resolver-Abfrageprotokollierung, Resolver-Regeln oder VPC-Endpunkte.
6. Wählen Sie auf der Registerkarte für die Ressource die Ressource aus, deren Zuordnung Sie aufheben möchten, und klicken Sie dann auf Zuordnung trennen.
7. Geben Sie im Dialogfeld Ressourcen trennen ein**`confirm`**, und wählen Sie dann Zuordnung trennen aus.

Mit einem Amazon Route 53 53-Profil VPCs verknüpfte Ansicht

Wählen Sie die Registerkarte Konsole, um Verbindungen zwischen Route 53 53-Profil und VPC anzuzeigen und zu bearbeiten. Wählen Sie die Registerkarte CLI, AWS CLI um Profile und VPC-Zuordnungen aufzulisten oder um Informationen zu einer bestimmten Zuordnung abzurufen

- Konsole
- CLI

Console

Zur Ansicht, die einem Profil VPCs zugeordnet ist

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie das Profil erstellt haben.
4. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, für das Sie das zugehörige Profil anzeigen möchten VPCs.
5. <Profile name>Wählen Sie auf der Seite die VPCsRegisterkarte aus.
6. Auf der Registerkarte für können VPCs Sie die Namen, den ARN und den Status für die zugehörigen anzeigen VPCs.

CLI

Sie können auflisten, mit denen VPCs das Profil verknüpft ist, indem Sie einen AWS CLI Befehl wie den folgenden ausführen:

```
aws route53profiles list-profile-associations
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",{
```

```
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

Sie können Informationen über einen bestimmten VPS abrufen, dem das Profil zugeordnet ist, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für `profile-association-id` verwenden:

`aws route53profiles get-profile-association --profile-association-id` **`rpassoc-489ce212fexample`**

Im Folgenden finden Sie eine Beispielausgabe, nachdem Sie den Befehl ausgeführt haben:

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
```

```
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Trennen einer VPC von einem Amazon Route 53 53-Profil

Wählen Sie eine Registerkarte, um ein Route 53 53-Profil mithilfe der Route 53-Konsole von einer VPC zu trennen, oder. AWS CLI

- Konsole
- CLI

Console

So trennen Sie die Zuordnung einer VPC, die einem Route 53 53-Profil zugeordnet ist

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der das Profil erstellt wurde, zu dem Sie eine VPC trennen möchten.
4. Wählen Sie die Schaltfläche neben dem Namen des Profils aus, zu dem Sie die Zuordnung einer VPC trennen möchten.
5. <Profile name>Wählen Sie auf der Seite die Registerkarte aus. VPCs
6. Wählen Sie auf der VPCs Registerkarte für die Ressource die VPC aus, deren Zuordnung Sie trennen möchten, und wählen Sie dann die Zuordnung aufheben.
7. Geben Sie im Dialogfeld „Ressourcen trennen“ ein, und wählen Sie dann Verknüpfung **`confirm`** trennen aus.

CLI

Sie können ein Profil von einer VPC trennen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für und verwenden: `profile-id` `--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

Im Folgenden finden Sie ein Beispiel für eine Ausgabe, nachdem Sie den Befehl ausgeführt haben:

```
"ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851401.362,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "DELETING",
        "StatusMessage": "Deleting Profile Association"
    }
```

Arbeiten mit gemeinsam genutzten Route 53 53-Profilen

Sie können ein Profil mit anderen Konten teilen, indem Sie:

- Erteilen Sie nur Leseberechtigungen, was bedeutet, dass das andere Konto das Profil seinem Konto zuordnen kann. VPCs In diesem Fall gelten alle DNS-Ressourcen und -Konfigurationen für die zugehörigen. VPCs
- Erteilung von Administratorberechtigungen. In diesem Fall können die Konten mit dem geteilten Profil das Profil ändern und es dann ihren Konten zuordnen VPCs. Ein Eigentümer kann auch vom Kunden verwaltete Berechtigungen erstellen, mit denen festgelegt werden kann, welche Aktionen vom Kundenkonto ausgeführt werden können. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Vom Kunden verwaltete Berechtigungen.

Amazon Route 53 Profile ist in AWS Resource Access Manager (AWS RAM) integriert, um die gemeinsame Nutzung von Ressourcen zu ermöglichen. AWS RAM ist ein Service, der es Ihnen ermöglicht, einige Route 53-Ressourcen mit anderen AWS-Konten oder über diese gemeinsam zu nutzen AWS Organizations. Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Zu den Verbrauchern können folgende Angaben zählen:

- Spezifisch AWS-Konten
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations

- Ihre gesamte Organisation ist in AWS Organizations

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

In diesem Thema wird erklärt, wie Sie Ressourcen teilen, deren Eigentümer Sie sind, und wie Sie Ressourcen verwenden, die mit Ihnen gemeinsam genutzt werden.

Inhalt

Erteilen von Berechtigungen für die gemeinsame Nutzung von Route 53 53-Profilen

Damit ein IAM-Prinzipal ein Profil gemeinsam nutzen kann, ist ein Mindestsatz an Berechtigungen erforderlich. Wir empfehlen die Verwendung der `AmazonRoute53ProfilesFullAccess` verwalteten IAM-Richtlinie, um sicherzustellen, dass Ihre IAM-Prinzipale über die erforderlichen Berechtigungen zum Teilen und Verwenden gemeinsam genutzter Profile verfügen.

Wenn Sie eine benutzerdefinierte IAM-Richtlinie verwenden, sind die Aktionen `route53profiles:GetProfilePolicy` und `route53profiles:PutProfilePolicy` erforderlich. Dies sind IAM-Aktionen, die nur für Berechtigungen gelten. Wenn einem IAM-Prinzipal diese Berechtigungen nicht erteilt wurden, tritt beim Versuch, das Profil mithilfe des Dienstes zu teilen, ein Fehler auf. AWS RAM

Voraussetzungen für die gemeinsame Nutzung von Route 53 53-Profilen

- Um ein Route 53 53-Profil zu teilen, müssen Sie es in Ihrem besitzen AWS-Konto. Das bedeutet, dass die Ressource Ihrem Konto zugewiesen oder bereitgestellt werden muss. Sie können kein Route 53 53-Profil teilen, das mit Ihnen geteilt wurde.

- Um ein Route 53 53-Profil mit Ihrer Organisation oder einer Organisationseinheit in zu teilen AWS Organizations, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM -Benutzerhandbuch.

Ein Route 53 53-Profil teilen

Wenn Sie ein Profil, das Sie besitzen, mit einem anderen teilen AWS-Konto, ermöglichen Sie es diesem, die DNS-bezogenen Einstellungen des Profils auf sein Profil anzuwenden. VPCs Dies macht es einfacher, einheitliche DNS-Konfigurationen für Tausende von Geräten VPCs mit minimalem Verwaltungsaufwand anzuwenden.

Um ein Route 53 53-Profil gemeinsam zu nutzen, müssen Sie es zu einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM -Ressource, mit der Sie Ihre Ressourcen in mehreren AWS-Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie ein Route 53 53-Profil über die Route 53-Konsole teilen, fügen Sie es einer vorhandenen Ressourcenfreigabe hinzu. Um das Route 53 53-Profil zu einer neuen Ressourcenfreigabe hinzuzufügen, müssen Sie zuerst die Ressourcenfreigabe mithilfe der AWS RAM Konsole erstellen.

Wenn Sie Teil einer Organisation in Ihrer Organisation sind AWS Organizations und das Teilen innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf das geteilte Route 53 53-Profil. Andernfalls erhalten Verbraucher eine Einladung, dem Resource Share beizutreten, und erhalten nach Annahme der Einladung Zugriff auf das gemeinsam genutzte Route 53 53-Profil.

Sie können mit der Freigabe eines Route 53 53-Profils, das Sie besitzen, auf der Route 53-Konsole beginnen und auf der AWS RAM Konsole fortfahren.

So geben Sie ein Route 53 53-Profil, das Sie besitzen, über die Route 53-Konsole frei

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie das Profil aus, das Sie teilen möchten, und wählen Sie auf der Seite mit den Profildetails die Option Profil teilen aus.
4. Sie werden zur AWS RAM Konsole weitergeleitet, wo Sie die folgenden Schritte ausführen können: Resource Share erstellen im AWS RAM Benutzerhandbuch.

5. Wenn ein Profil für Sie freigegeben wurde, enthält die Tabelle Profile den Text Für mich freigegeben.

   Wenn Sie ein Profil geteilt haben, wird es in der Tabelle Profile als Gemeinsam genutzt aufgeführt.

So geben Sie ein Route 53 53-Profil, das Sie besitzen, über die AWS RAM Konsole frei

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

So teilen Sie ein Route 53 53-Profil, das Sie besitzen, mit dem AWS CLI

Verwenden Sie den Befehl create-resource-share.

Aufheben der Freigabe eines geteilten Route 53 53-Profils

Wenn Sie die Freigabe eines Profils aufheben und VPCs denen die Konfigurationen dieses Profils zugeordnet sind, gehen diese verloren und es werden standardmäßig die VPC-spezifischen Konfigurationen verwendet.

Um die Freigabe eines gemeinsam genutzten Route 53 53-Profils, das Ihnen gehört, aufzuheben, müssen Sie es aus der Ressourcenfreigabe entfernen. Sie können dies mit der Route 53-Konsole, der AWS RAM Konsole oder dem AWS CLI tun.

So heben Sie die Freigabe eines geteilten Route 53 53-Profils, das Sie besitzen, mithilfe der Route 53-Konsole auf

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wählen Sie den verknüpften Namen des Profils aus, dessen Freigabe Sie rückgängig machen möchten, und <Profile name>wählen Sie auf der Seite die Option Teilen verwalten aus.
4. Sie werden zur AWS RAM Konsole weitergeleitet, auf der Sie die folgenden Schritte ausführen können: Aktualisierung einer Ressourcenfreigabe im AWS RAM Benutzerhandbuch.

So heben Sie die Freigabe eines geteilten Route 53 53-Profils, das Sie besitzen, mithilfe der Konsole auf AWS RAM

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die Freigabe eines geteilten Route 53 53-Profils aufzuheben, das Ihnen gehört, verwenden Sie den AWS CLI

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren eines gemeinsamen Route 53 53-Profils

Besitzer und Verbraucher können gemeinsam genutzte Route 53 53-Profile mithilfe der Route 53-Konsole identifizieren und AWS CLI.

So identifizieren Sie ein gemeinsam genutztes Route 53 53-Profil mithilfe der Route 53-Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich Profile aus.
3. Wenn ein Profil für Sie freigegeben wurde, enthält die Tabelle Profile den Text Für mich freigegeben.

   Wenn Sie ein Profil geteilt haben, wird es in der Tabelle Profile als Gemeinsam genutzt aufgeführt.

Um ein gemeinsam genutztes Route 53 53-Profil zu identifizieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl get-profile oder den Befehl list-profile. Die Befehle geben Informationen zu den Route 53 53-Profilen zurück, die Sie besitzen, und zum Freigabestatus der Route 53 53-Profile.

Zuständigkeiten und Berechtigungen für gemeinsam genutzte Route 53 53-Profile

Berechtigungen für Besitzer

Ein Profilbesitzer kann Profilressourcenzuordnungen anzeigen, verwalten und löschen, einschließlich der von den Benutzerkonten erstellten Ressourcenzuordnungen. Der Besitzer kann die VPC-Zuordnungen, die er besitzt, anzeigen und löschen. Darüber hinaus kann nur ein Profilbesitzer ein Profil löschen, das ihm gehört. Dadurch werden auch automatisch alle Ressourcenzuordnungen des Profils entfernt.

> **Note**
>
> Sie müssen eine benutzerdefinierte verwaltete Berechtigung erstellen, die zusätzlich zu den Standardberechtigungen die `route53profiles:AssociateResourceToProfile` Aktion umfasst, Ressourcen aus den Konten zuzuordnen, für die das Profil freigegeben ist, da dies in der Standardrichtlinie `AWSRAMPermissionRoute53ProfileAllowAssociation` nicht enthalten ist.

Berechtigungen für Konsumenten

Die Standardberechtigung für Nutzer eines geteilten Profils ist schreibgeschützt. Mit Leseberechtigungen können sie die zugehörigen Ressourcen sehen und ihnen zuordnen VPCs, sie können die Ressourcenzuordnungen jedoch nicht verwalten.

Ein Besitzer kann auch vom Kunden verwaltete Berechtigungen auf der AWS RAM Konsole erstellen. Weitere Informationen finden Sie im AWS RAM Benutzerhandbuch unter Vom Kunden verwaltete Berechtigungen erstellen und verwenden.

Fakturierung und Messung

Route 53 53-Profile werden auf der Grundlage der Anzahl der VPC-Zuordnungen abgerechnet. Der Profilinhaber ist für die Abrechnung der VPC-Zuordnungen durch den Kunden verantwortlich.

Kontingente für Instanzen

Die Profilbesitzer und Verbraucher teilen sich dasselbe Kontingent, mit Ausnahme der Anzahl von Route 53 53-Profilen pro Konto in einer Region. Weitere Informationen finden Sie unter Kontingente für Route 53 53-Profile .

Was ist Amazon Route 53 auf Outposts?

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastrukturen APIs, Dienste und Tools auf Kundenstandorte ausdehnt. Auf diese Weise können Kunden AWS Dienste mit lokalen Workloads ausführen, indem sie dieselben Programmierschnittstellen wie in verwenden. AWS-Regionen Weitere Informationen finden Sie unter Was ist? AWS Outposts im AWS Outposts Benutzerhandbuch.

Route 53 auf Outposts bietet zwei Funktionen:

- Ein VPC-Resolver, der alle DNS-Abfragen zwischenspeichert, die von der stammen. AWS Outposts
- Hybridkonnektivität zwischen einem Outpost und einem On-Premises-DNS-Resolver, wenn Sie ein- und ausgehende Endpunkte bereitstellen.

Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.

Darüber hinaus reduziert Route 53 auf Outposts die Netzwerklatenz, da Abfragen innerhalb des Outposts und somit ohne Roundtrip zur nächstgelegenen AWS-Region aufgelöst werden können.

- Ein VPC-Resolver, der alle DNS-Abfragen zwischenspeichert, die von der stammen. AWS Outposts
- Hybridkonnektivität zwischen einem Outpost und einem On-Premises-DNS-Resolver, wenn Sie ein- und ausgehende Endpunkte bereitstellen.

Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.

Darüber hinaus reduziert Route 53 auf Outposts die Netzwerklatenz, da Abfragen innerhalb des Outposts und somit ohne Roundtrip zur nächstgelegenen AWS-Region aufgelöst werden können.

> **Note**
>
> Wenn Sie eine Version von AWS Outposts Racks haben, die nicht mit Route 53 auf Outposts kompatibel ist, wird ein AWS Account-Team benachrichtigt und wird sich mit Ihnen in Verbindung setzen, um Ihnen beim Upgrade AWS Outposts zu helfen.

Übersicht über die Architektur

Route 53 on Outposts implementiert eine verteilte DNS-Architektur:

- DNS-Einträge und gehostete Zonen bleiben in Amazon Route 53 in der AWS Region verwaltet
- Die Resolver-Funktionalität erstreckt sich auf Ihr AWS Outposts Rack und ermöglicht die lokale Verarbeitung von Abfragen

Dieses Design optimiert die Abfrageleistung und Verfügbarkeit und sorgt gleichzeitig für eine zentrale DNS-Datensatzverwaltung. DNS-Einträge werden weiterhin in der AWS Region gespeichert, nicht lokal im AWS Outposts Rack.

Features von Amazon Route 53 auf Outposts

In der folgenden Tabelle werden die Features von Route 53 auf Outposts mit den Features von Amazon Route 53 verglichen.

Route 53 auf Outposts im Vergleich zu Route 53

Feature	Verfügbarkeit in Route 53 auf Outposts
VPC-Resolver	Ja. VPC Resolver verwaltet einen lokalen Cache mit Datensätzen für Anwendungen, die auf dem Outpost-Rack gehostet werden, für die Peering-VPC im und für alle öffentlich AWS-Region zugänglichen Hostnamen.
Health checks (Zustandsprüfungen)	Nein. Zustandsprüfungen werden über die AWS-Region berechnet und gemeldet. Wenn ein Outpost die Cloud-Verbindung trennt, können die Endpunkte nicht geöffnet werden und es kann kein Failover auf eine Sicherung durchgeführt werden.
Resolver-Endpunkte	Ja. Resolver-Endpunkte im Outpost-Rack ermöglichen die Weiterleitung und den Empfang von DNS-Abfragen von On-Premises-DNS-Servern. Nur der IPv4 Endpunkttyp ist für Endpoints verfügbar.

Feature	Verfügbarkeit in Route 53 auf Outposts
Resolver, DNS-Firewall	Nicht verfügbar.
Datenverkehrsfluss	Nicht verfügbar.

Verhalten des VPC-Resolvers, wenn die Verbindung zur VPC getrennt AWS Outposts wird

Wenn die Verbindung zum AWS Outposts unterbrochen wird AWS-Region, verhält sich der Resolver auf Outpost wie folgt:

- Änderungen auf Steuerebene sind nicht verfügbar.
- Zustandsprüfungen und DNS-Failover-Funktionen sind nicht verfügbar.
- DNS-Abfragen für Ressourcen, die lokal in den Outposts gehostet werden, werden zwar aufgelöst, aber in einigen Fällen ist die Antwort möglicherweise veraltet, wenn die IP-Adresse für die Ressource aktualisiert wurde, während der Outpost nicht verbunden war.
- DNS-Abfragen für Ressourcen, die in der regionsinternen VPC gehostet werden, können aufgelöst werden. Auf die Ressourcen kann jedoch erst zugegriffen werden, wenn die Outpost-Verbindung mit der AWS-Region wiederhergestellt wurde.
- DNS-Abfragen für öffentliche DNS-Ressourcen können gelöst werden, wenn sie im VPC Resolver-Cache auf Outpost verfügbar sind.

Erste Schritte mit VPC Resolver on AWS Outposts

Nachdem Sie Ihre AWS Outposts Racks bestellt haben und sie geliefert wurden, wie hier beschrieben: Erstellen Sie ein AWS Outposts im AWS Outposts Leitfaden, können Sie Resolver auf Outpost einrichten.

> **Important**
>
> Resolver on Outpost kann nur von dem AWS Konto erstellt werden, dem das Rack gehört. AWS Outposts Wenn das AWS Outposts Rack mit anderen Konten geteilt wird, können diese Konten keinen Resolver on Outpost auf dem gemeinsam genutzten Rack erstellen.

Sie können es auch verwenden APIs , um Route 53 auf Outposts zu verwalten. Weitere Informationen finden Sie unter Aktionen für Resolver auf Outpost.

> **Important**
>
> Es kann bis zu 30-150 Minuten dauern, einen VPC-Resolver-Cache auf einem zu erstellen. AWS Outposts

Nachdem Sie Ihre AWS Outposts Racks geliefert haben, können Sie sich für Route 53 on Outposts entscheiden.

So konfigurieren Sie Resolver auf Outpost

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Wählen Sie auf der Seite Resolver on Outpost die Option Create VPC Resolver aus.
5. Gehen Sie auf der Seite „VPC Resolver erstellen“ wie folgt vor:

   - AWS OutpostsWählen Sie unter aus, auf dem AWS Outposts Sie den VPC-Resolver erstellen möchten.
   - Geben Sie einen Namen für den VPC-Resolver in das Textfeld VPC-Resolver-Name ein.
   - Nachdem die empfohlenen Instance-Typen für VPC Resolver mit EC2 Amazon-Instances gefüllt wurden, wählen Sie eine aus.

     Weitere Informationen zu den Instance-Typen finden Sie unter Kontingente für Resolver auf Outpost.
   - Wählen Sie unter Anzahl der Instances die Anzahl der Elastic Interface-Instances für den VPC VPC Resolver aus. Der Standardwert ist „4“.

     Wenn Sie AWS Outposts keinen Instance-Typ haben, der VPC Resolver unterstützt, können Sie keinen VPC Resolver erstellen.
6. Wählen Sie Create VPC Resolver aus.

Sie können die Erstellung des VPC-Resolvers auf der Seite Resolver on Outpost überwachen.

Erstellen eingehender Endpunkte

Nachdem Sie eine Instance von Resolver auf Outpost erstellt haben, können Sie sowohl ein- als auch ausgehende Endpunkte hinzufügen, um ein- und ausgehende DNS-Abfragen Ihres On-Premises-Netzwerks aufzulösen.

So konfigurieren Sie eingehende Endpunkte für Resolver auf Outpost

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Details anzeigen aus.
5. Wählen Sie in der Tabelle Eingehende Endpunkte die Option Eingehenden Endpunkt erstellen aus.
6. Geben Sie auf der Seite Eingehenden Endpunkt erstellen die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die beim Erstellen oder Bearbeiten eingehender Endpunkte auf einem Outpost angegeben werden.
7. Wählen Sie Endpunkt erstellen aus.

Werte, die beim Erstellen oder Bearbeiten eingehender Endpunkte auf einem Outpost angegeben werden

Wenn Sie einen eingehenden Endpunkt erstellen oder bearbeiten, geben Sie die folgenden Werte an:

ID des Außenpostens

Wenn Sie den Endpunkt für einen VPC-Resolver auf einer AWS Outposts VPC erstellen, ist dies die ID. AWS Outposts

Endpoint name (Endpunktname)

Ein Anzeigename, mit dem Sie ganz einfach einen eingehenden Endpunkt auf dem Dashboard finden können.

VPC in der Region region-name

Alle eingehenden DNS-Anfragen aus Ihrem Netzwerk passieren diese VPC auf dem Weg zum VPC Resolver.

Sicherheitsgruppe für diesen Endpunkt

Die ID einer oder mehrerer Sicherheitsgruppen, die Sie verwenden möchten, um den Zugriff auf diesen eingehenden Endpunkt zu kontrollieren. Die von Ihnen angegebene Sicherheitsgruppe muss eine oder mehrere eingehende Regeln enthalten. Eingehende Regeln müssen TCP- und UDP-Zugriff auf Port 53 zulassen. Sie können diesen Wert nicht ändern, nachdem Sie einen Endpunkt erstellt haben.

Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für Ihre VPC im Amazon VPC-Benutzerhandbuch.

IP-Adressen

Die IP-Adressen, die Sie den eingehenden Endpunkten zuweisen möchten. Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben. Beachten Sie Folgendes:

IP-Adressen und Amazon VPC Elastic Network-Schnittstellen

Für jede Kombination aus Availability Zone, Subnetz und IP-Adresse, die Sie angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente auf Route 53 VPC Resolver. Informationen zu den Preisen für die einzelnen Elastic-Network-Schnittstellen finden Sie auf der Seite Amazon Route 53 – Preise unter „Amazon Route 53“.

> **Note**
>
> Der Resolver-Endpunkt hat eine private IP-Adresse. Diese IP-Adressen ändern sich im Laufe der Lebensdauer eines Endpunkts nicht.

Geben Sie für jede IP-Adresse die folgenden Werte an. Jede IP-Adresse muss in einer Availability Zone in der VPC vorhanden sein, die Sie in VPC in der Region region-name angegeben haben.

Availability Zone

Die Availability Zone, die DNS-Abfragen auf dem Weg zu Ihrer VPC durchlaufen sollen. Die angegebene Availability Zone muss mit einem Subnetz konfiguriert sein.

Subnetz

Das Subnetz, das die IP-Adresse enthält, an die DNS-Abfragen weitergeleitet werden sollen. Das Subnetz muss eine verfügbare IP-Adresse enthalten.

Geben Sie das Subnetz für eine Adresse an. IPv4 IPv6 wird nicht unterstützt.

IP-Adresse

Die IP-Adresse in Ihrem Netzwerk, an die DNS-Abfragen weitergeleitet werden sollen.

Wählen Sie aus, ob VPC Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst angeben möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie eine Adresse ein. IPv4 IPv6 wird nicht unterstützt.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Dies sind die Tags, AWS Fakturierung und Kostenmanagement mit denen Sie Ihre AWS Rechnung organisieren können. Sie können Tags auch für andere Zwecke verwenden. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

Erstellen ausgehender Endpunkte

Nachdem Sie sich für einen VPC-Resolver angemeldet und ihn konfiguriert haben, können Sie auch sowohl eingehende als auch ausgehende Endpunkte hinzufügen, um DNS-Abfragen in Ihrem lokalen Netzwerk zu lösen.

> **Note**
>
> Wenn Sie ausgehende Endpunkte konfigurieren, speichert VPC Resolver DNS-Antworten im Cache, sodass Anfragen auch dann gelöst werden können, wenn Ihr Outpost von der Region getrennt wird. Die Wartung dieses Caches kann zu einer Zunahme der DNS-Anfragen an Ihre lokalen Resolver führen.

So konfigurieren Sie ausgehende Endpunkte für Resolver auf Outpost

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Wählen Sie das Häkchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Details anzeigen aus.
5. Wählen Sie in der Tabelle Ausgehende Endpunkte die Option Ausgehenden Endpunkt erstellen aus.
6. Geben Sie auf der Seite Eingehenden Endpunkt erstellen die entsprechenden Werte ein. Weitere Informationen finden Sie unter Werte, die beim Erstellen oder Bearbeiten ausgehender Endpunkte in einer Instance von AWS Outposts angegeben werden.
7. Wählen Sie Endpunkt erstellen aus.

Werte, die beim Erstellen oder Bearbeiten ausgehender Endpunkte in einer Instance von AWS Outposts angegeben werden

Wenn Sie einen ausgehenden Endpunkt erstellen oder bearbeiten, geben Sie die folgenden Werte an:

ID des Außenpostens

Wenn Sie den Endpunkt für einen VPC-Resolver auf einer AWS Outposts VPC erstellen, ist dies die ID. AWS Outposts

Endpoint name (Endpunktname)

Ein Anzeigename, mit dem Sie ganz einfach einen ausgehenden Endpunkt auf dem Dashboard finden können.

VPC in der Region region-name

Alle ausgehenden DNS-Anfragen von Ihrer VPC passieren diese VPC auf dem Weg zu Ihrem Netzwerk.

Sicherheitsgruppe für diesen Endpunkt

Die ID einer oder mehrerer Sicherheitsgruppen, die Sie verwenden möchten, um den Zugriff auf diese VPC zu steuern. Die von Ihnen angegebene Sicherheitsgruppe muss eine oder mehrere ausgehende Regeln enthalten. Ausgehende Regeln müssen TCP- und UDP-Zugriff auf dem Port zulassen, den Sie für DNS-Abfragen in Ihrem Netzwerk verwenden. Sie können diesen Wert nicht ändern, nachdem Sie einen Endpunkt erstellt haben.

Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für Ihre VPC im Amazon VPC-Benutzerhandbuch.

IP-Adressen

Die IP-Adressen, die Sie den ausgehenden Endpunkten zuweisen möchten. Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben. Beachten Sie Folgendes:

IP-Adressen und Amazon VPC Elastic Network-Schnittstellen

Für jede Kombination aus Availability Zone, Subnetz und IP-Adresse, die Sie angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente auf Route 53 VPC Resolver. Weitere Informationen zu den Preisen für die einzelnen Elastic Network-Schnittstellen finden Sie unter "Amazon Route 53" auf der Seite Amazon Route 53 Preise.

> **Note**
>
> Der Resolver-Endpunkt hat eine private IP-Adresse. Diese IP-Adressen ändern sich im Laufe der Lebensdauer eines Endpunkts nicht.

Geben Sie für jede IP-Adresse die folgenden Werte an. Jede IP-Adresse muss in einer Availability Zone in der VPC vorhanden sein, die Sie in VPC in der Region region-name angegeben haben.

Availability Zone

Die Availability Zone, die DNS-Abfragen auf dem Weg von Ihrer VPC passieren sollen. Die angegebene Availability Zone muss mit einem Subnetz konfiguriert sein.

Subnetz

Das Subnetz, das die IP-Adresse enthält, von der aus Sie DNS-Anfragen weiterleiten möchten. Das Subnetz muss eine verfügbare IP-Adresse enthalten.

Geben Sie das Subnetz für eine Adresse an IPv4 . IPv6 wird nicht unterstützt.

IP-Adresse

Die IP-Adresse, die Sie den ausgehenden Endpunkten zuweisen möchten.

Wählen Sie aus, ob VPC Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst angeben möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie eine Adresse ein. IPv4 IPv6 wird nicht unterstützt.

Tags (Markierungen)

Geben Sie einen oder mehrere Schlüssel und die entsprechenden Werte an. Sie können z. B. Cost center (Kostenstelle) als Key (Schlüssel) und 456 als Value (Wert) angeben.

Dies sind die Tags, mit AWS Fakturierung und Kostenmanagement denen Sie Ihre AWS Rechnung organisieren können. Sie können Tags auch für andere Zwecke verwenden. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

Erstellen von Weiterleitungsregeln für ausgehende Endpunkte

Sie können auch Weiterleitungsregeln für ausgehende Endpunkte erstellen. Weitere Informationen finden Sie unter Um Weiterleitungsregeln zu erstellen und die Regeln einer oder mehreren zuzuordnen VPCs.

Verwalten von Resolver auf Outpost

Führen Sie zum Verwalten von Resolver auf Outpost die entsprechenden Schritte aus.

Themen

Bearbeiten von Resolver auf Outpost

Gehen Sie wie folgt vor, um einen Resolver auf Outpost zu bearbeiten.

So bearbeiten Sie einen Resolver auf Outpost

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Markieren Sie das Häkchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Bearbeiten.
5. Folgende Informationen können bearbeitet werden:
   - Der Name des VPC-Resolvers
   - Der Instance-Typ
   - Die Anzahl der -Instances
6. Wählen Sie Änderungen speichern aus, wenn Sie mit der Bearbeitung fertig sind.

Anzeigen des Status von Resolver auf Outpost

Gehen Sie wie folgt vor, um den Status für Resolver auf Outpost anzuzeigen.

So zeigen Sie den Status eines eingehenden Endpunkts an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Wählen Sie das Häkchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Details anzeigen aus.
5. Die Spalte Status auf der Seite Resolver auf Outpost enthält einen der folgenden Werte:

   Erstellen

   Der Resolver auf Outpost wird gerade erstellt.

   Betriebsbereit

   Der Resolver auf Outpost ist korrekt konfiguriert.

   Aktualisieren

   Der Resolver auf Outpost aktualisiert Instance-Typen.

   Aktion erforderlich

   Dieser VPC-Resolver ist fehlerhaft und kann nicht automatisch wiederhergestellt werden. Um das Problem zu lösen, empfehlen wir Ihnen, sicherzustellen, dass die Instance Resolver auf AWS Outposts Outpost unterstützt.

   Löschen

   Der Resolver auf Outpost wird gerade gelöscht.

   Erstellen fehlgeschlagen

   Die Erstellung von Resolver auf Outpost war nicht erfolgreich.

   Fehler beim Löschen

   Die Löschung von Resolver auf Outpost war nicht erfolgreich. Versuchen Sie es in ein paar Minuten erneut, um dieses Problem zu beheben.

Löschen von Resolver auf Outpost

> **Note**
>
> Um einen Resolver auf Outpost löschen zu können, müssen zunächst alle damit verbundenen Endpunkte gelöscht werden.

Gehen Sie wie folgt vor, um einen Resolver auf Outpost zu löschen.

So löschen Sie einen Resolver auf Outpost

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Löschen.
5. Geben Sie im Dialogfeld VPC Resolver löschen den Text **`delete`** in das Textfeld ein und wählen Sie Löschen aus.

Verwalten eingehender Endpunkte für Resolver auf Outpost

Führen Sie zum Verwalten eingehender Endpunkte für Resolver auf Outpost die entsprechenden Schritte aus.

Themen

Anzeigen und Bearbeiten von eingehenden Endpunkten

Führen Sie zum Anzeigen und Bearbeiten von Einstellungen für einen eingehenden Endpunkt die folgenden Schritte aus.

Anzeigen und Bearbeiten von Einstellungen für einen eingehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebszustand befindet, und wählen Sie Details anzeigen aus.
5. Wählen Sie in der Liste Eingehende Endpunkte die Option für den Endpunkt aus, für den Sie Einstellungen anzeigen oder den Sie bearbeiten möchten.
6. Wählen Sie View details (Details anzeigen) oder Edit (Bearbeiten).

   Informationen zu den Werten für eingehende Endpunkte finden Sie unter Werte, die beim Erstellen oder Bearbeiten ausgehender Endpunkte in einer Instance von AWS Outposts angegeben werden.
7. Wenn Sie Edit (Bearbeiten) gewählt haben, geben Sie die entsprechenden Werte ein und klicken Sie anschließend auf Save (Speichern).

Anzeigen des Status für eingehende Endpunkte

Gehen Sie folgendermaßen vor, um den Status eines eingehenden Endpunkts anzuzeigen.

So zeigen Sie den Status eines eingehenden Endpunkts an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebsstatus befindet, und wählen Sie Details anzeigen aus.
5. Die Spalte Status der Liste Eingehende Endpunkte enthält einen der folgenden Werte:

Erstellen

VPC Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

Betriebsbereit

Die Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt sind korrekt konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und VPC Resolver weiterleiten.

Aktualisieren

Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

Automatische Wiederherstellung

VPC Resolver versucht, eine oder mehrere der Netzwerkschnittstellen wiederherzustellen, die diesem Endpunkt zugeordnet sind. Während der Wiederherstellung funktioniert der Endpunkt aufgrund des Limits für die Anzahl der DNS-Abfragen pro IP-Adresse (pro Netzwerkschnittstelle) mit begrenzter Kapazität. Das aktuelle Limit finden Sie unter Kontingente auf Route 53 VPC Resolver.

Aktion erforderlich

Dieser Endpunkt ist fehlerhaft und VPC Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zugeordnet haben. Fügen Sie für jede IP-Adresse, die nicht verfügbar ist, eine andere IP-Adresse hinzu und löschen Sie dann die nicht verfügbare IP-Adresse. Ein Endpunkt muss immer mindestens zwei IP-Adressen enthalten. Ein Status von Aktion erforderlich kann verschiedene Ursachen haben. Hier sind zwei häufige Ursachen:

- Eine oder mehrere Netzwerkschnittstellen, die diesem Endpunkt zugeordnet sind, wurden mit Amazon VPC gelöscht.
- Die Netzwerkschnittstelle konnte aus irgendeinem Grund nicht erstellt werden, der außerhalb der Kontrolle von VPC Resolver liegt.

Löschen

Resolver löscht diesen Endpunkt und die zugehörigen Netzwerkschnittstellen.

Löschen von eingehenden Endpunkten

Gehen Sie wie folgt vor, um einen eingehenden Endpunkt zu löschen.

> **Important**
>
> Wenn Sie einen eingehenden Endpunkt löschen, werden DNS-Anfragen aus Ihrem Netzwerk nicht mehr an den VPC Resolver in der VPC weitergeleitet, die Sie im Endpunkt angegeben haben.

So löschen Sie einen eingehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebsstatus befindet, und wählen Sie Details anzeigen aus.
5. Aktivieren Sie das Kontrollkästchen neben dem zu löschenden Endpunkt.
6. Wählen Sie Löschen aus.
7. Um zu bestätigen, dass Sie den Endpunkt löschen möchten, geben Sie den Namen des Endpunkts ein und wählen Sie Submit (Senden).

Verwalten ausgehender Endpunkte für Resolver auf Outpost

Führen Sie zum Verwalten ausgehender Endpunkte für Resolver auf Outpost die entsprechenden Schritte aus.

Themen

Anzeigen und Bearbeiten von ausgehenden Endpunkten

Führen Sie zum Anzeigen und Bearbeiten von Einstellungen für einen ausgehenden Endpunkt die folgenden Schritte aus.

Anzeigen und Bearbeiten von Einstellungen für einen ausgehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.
4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebsstatus befindet, und wählen Sie Details anzeigen aus.
5. Wählen Sie in der Liste Ausgehende Endpunkte das Kontrollkästchen neben dem Endpunkt aus, für den Sie Einstellungen anzeigen oder den Sie bearbeiten möchten.
6. Wählen Sie View details (Details anzeigen) oder Edit (Bearbeiten).

   Informationen zu den Werten für ausgehende Endpunkte finden Sie unter Werte, die beim Erstellen oder Bearbeiten ausgehender Endpunkte in einer Instance von AWS Outposts angegeben werden.
7. Wenn Sie Edit (Bearbeiten) gewählt haben, geben Sie die entsprechenden Werte ein und klicken Sie anschließend auf Save (Speichern).

Anzeigen des Status für ausgehende Endpunkte

Gehen Sie folgendermaßen vor, um den Status eines ausgehenden Endpunkts anzuzeigen.

So zeigen Sie den Status eines ausgehenden Endpunkts an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie AWS Outposts sich befinden.

4. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebsstatus befindet, und wählen Sie Details anzeigen aus.
5. In der Liste Ausgehende Endpunkte enthält die Spalte Status einen der folgenden Werte:

   Erstellen

   VPC Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

   Betriebsbereit

   Die Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt sind korrekt konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und VPC Resolver weiterleiten.

   Aktualisieren

   Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

   Automatische Wiederherstellung

   VPC Resolver versucht, eine oder mehrere der Netzwerkschnittstellen wiederherzustellen, die diesem Endpunkt zugeordnet sind. Während der Wiederherstellung funktioniert der Endpunkt aufgrund des Limits für die Anzahl der DNS-Abfragen pro IP-Adresse (pro Netzwerkschnittstelle) mit begrenzter Kapazität. Das aktuelle Limit finden Sie unter Kontingente auf Route 53 VPC Resolver.

   Aktion erforderlich

   Dieser Endpunkt ist fehlerhaft und VPC Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zugeordnet haben. Fügen Sie für jede IP-Adresse, die nicht verfügbar ist, eine andere IP-Adresse hinzu und löschen Sie dann die nicht verfügbare IP-Adresse. (Ein Endpunkt muss immer mindestens zwei IP-Adressen enthalten.) Ein Status von Aktion erforderlich kann verschiedene Ursachen haben. Hier sind zwei häufige Ursachen:

   - Eine oder mehrere Netzwerkschnittstellen, die diesem Endpunkt zugeordnet sind, wurden mit Amazon VPC gelöscht.
   - Die Netzwerkschnittstelle konnte aus irgendeinem Grund nicht erstellt werden, der außerhalb der Kontrolle von VPC Resolver liegt.

Löschen

Resolver löscht diesen Endpunkt und die zugehörigen Netzwerkschnittstellen.

Löschen von ausgehenden Endpunkten

Bevor Sie einen Endpunkt löschen können, müssen Sie zunächst alle Regeln löschen, die einer VPC zugeordnet sind.

Gehen Sie wie folgt vor, um einen ausgehenden Endpunkt zu löschen.

> **Important**
>
> Wenn Sie einen ausgehenden Endpunkt löschen, beendet VPC Resolver die Weiterleitung von DNS-Anfragen von Ihrer VPC an Ihr Netzwerk für Regeln, die den gelöschten ausgehenden Endpunkt angeben.

So löschen Sie einen ausgehenden Endpunkt

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie im linken Navigationsbereich die Option Resolver und navigieren Sie dann zu Outposts.
3. Aktivieren Sie das Kontrollkästchen neben dem VPC-Resolver, der sich im Betriebsstatus befindet, und wählen Sie Details anzeigen aus.
4. Wählen Sie in der Liste Ausgehende Endpunkte die Option für den zu löschenden Endpunkt aus.
5. Wählen Sie Löschen aus.
6. Um zu bestätigen, dass Sie den Endpunkt löschen möchten, geben Sie den Namen des Endpunkts ein und wählen Sie dann Submit (Senden).

Was ist Route 53 Global Resolver?

Route 53 Global Resolver ist ein über das Internet erreichbarer DNS-Resolver, der eine einfache, sichere und zuverlässige DNS-Auflösung für autorisierte Kunden in Ihrem Unternehmen an entfernten Standorten, Zweigstellen und lokalen Umgebungen bietet. Sie können Anfragen für Domains lösen, die auf privaten Hosting-Zonen von Amazon Route 53 oder öffentlichen Domains im Internet gehostet werden, und gleichzeitig die hohe Verfügbarkeit durch die globale Anycast-Architektur aufrechterhalten. Route 53 Global Resolver hilft Ihnen, Ihre Kunden vor DNS-basierten Datenexfiltrationsangriffen zu schützen, indem Anfragen an potenziell bösartige Domänen gefiltert werden.

Route 53 Global Resolver verwendet Anycast-IP-Adressen, die DNS-Abfragen automatisch an die AWS Region weiterleiten, die Ihrem Quellabfrageort am nächsten liegt, um eine optimale Latenz und Verfügbarkeit zu gewährleisten. Sie können die Regionen auswählen, in denen Ihr globaler Resolver die DNS-Auflösung für Ihre autorisierten Clients bereitstellen soll, verschiedene Ansichten für die Clients für die Auflösung von privaten und öffentlichen Domänen konfigurieren, bösartige Domänen filtern und die DNS-Aktivitäten in Ihrer gesamten Organisation überwachen.

Themen

- Kontingente für Route 53 Global Resolver

Warum Route 53 Global Resolver?

Route 53 Global Resolver bietet zentralisierte DNS-Sicherheit und Filterung für Remote- und Hybrid-Clients und Workloads an mehreren Standorten. Unabhängig vom Standort Ihrer Workloads, Anwendungen oder Benutzer gewährleistet Route 53 Global Resolver einen konsistenten DNS-Schutz, ohne dass eine komplexe lokale Infrastruktur erforderlich ist.

Hauptvorteile für Remote- und Hybridumgebungen:

- Vereinfachtes Management — Konfigurieren Sie die Auflösung privater und öffentlicher Domänen mit einer einzigen Lösung, anstatt mehrere lokale DNS-Server zu verwalten
- Einheitliche DNS-Sicherheit — Wenden Sie konsistente Filterrichtlinien für alle Remote-Clients und hybriden Workloads an
- Skalierbarer Schutz — Wird automatisch skaliert, um DNS-Anfragen von wachsenden Remote-Mitarbeitern und Cloud-Workloads zu verarbeiten
- Reduzierte Infrastruktur — Minimiert den Bedarf an DNS-Sicherheitsgeräten an jedem Remote-Standort

Informationen zu den ersten Schritten finden Sie unter:

- the section called “Konzepte und Terminologie”- Kernkonzepte für die Bereitstellung von DNS-Sicherheit
- the section called “Funktionsweise”- So schützt Route 53 Global Resolver Remote- und Hybridumgebungen
- the section called “Tutorial: Erstellen Sie Ihren ersten Route 53 Global Resolver”- Tutorial für Ihr erstes DNS-Filter-Setup

Wichtige Konzepte und Komponenten für Route 53 Global Resolver

Route 53 Global Resolver verwendet mehrere Schlüsselkomponenten, die zusammenarbeiten, um DNS-Auflösung mit geteiltem Traffic, hohe Verfügbarkeit durch globale Anycast-Architektur und umfassende DNS-Sicherheit für Ihr Unternehmen zu gewährleisten. Das Verständnis dieser Route 53 Global Resolver-Konzepte hilft Ihnen bei der Entwicklung und Bereitstellung von Lösungen, die

einen nahtlosen Zugriff auf private und öffentliche Ressourcen ermöglichen, die Servicekontinuität über mehrere Regionen hinweg sicherstellen und vor DNS-basierten Bedrohungen schützen.

DNS-Resolver für Kunden vor Ort und an entfernten Standorten

Um Route 53 Global Resolver für Ihre verteilten Workloads, Kundenstandorte und Benutzer bereitzustellen, konfigurieren Sie diese Schlüsselkomponenten:

Globaler Resolver

: Die Hauptdienstinstanz, die DNS-Auflösung und Filterung für Ihr Unternehmen in mehreren AWS Regionen bereitstellt. Ihr globaler Resolver verwendet die Anycast-Technologie, um DNS-Anfragen automatisch an die nächstgelegene verfügbare Region weiterzuleiten und so schnelle Antwortzeiten für alle Kunden unabhängig von ihrem Standort zu gewährleisten.

Anycast-IP-Adressen

: Zwei eindeutige IPv4 oder IPv6 Adressen, die Ihrem globalen Resolver zugewiesen sind und den Sie auf Client-Geräten und Netzwerkgeräten konfigurieren. Diese Anycast-IP-Adressen sind weltweit identisch, was die DNS-Konfiguration an all Ihren Standorten vereinfacht. Die Anycast-IP-Adressierung ermöglicht das automatische Routing von DNS-Anfragen an den nächstgelegenen globalen Resolver, wodurch die Antwortzeiten optimiert und die Zuverlässigkeit der Dienste verbessert werden.

DNS-Ansichten

: Konfigurationsvorlagen, mit denen Sie unterschiedliche DNS-Richtlinien auf verschiedene Gruppen von Clients in Ihrem Netzwerk anwenden können. Verwenden Sie DNS-Ansichten, um Split-Horizon-DNS zu implementieren. Wenden Sie beispielsweise strenge Filter und Token-Authentifizierung für entfernte Standorte an, während Sie IP-basierten Zugriff und unterschiedliche Sicherheitsrichtlinien für Zweigstellen verwenden.

DNS-Client-Authentifizierung

Wählen Sie die Authentifizierungsmethode aus, die für Ihre Bereitstellung am besten geeignet ist:

Tokenbasierte Authentifizierung

: Sichere DNS-Verbindungen mit verschlüsselten Tokens für DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT). Sie können eindeutige Zugriffstoken für einzelne Clients oder Gerätegruppen generieren, Ablaufzeiträume festlegen und Token nach Bedarf widerrufen.

Greifen Sie auf quellenbasierte Authentifizierung zu

Steuern Sie den Zugriff mithilfe von IP-Adressen und Zulassungslisten für CIDR-Bereiche. Sie können die öffentlichen IP-Adressen oder Netzwerkbereiche Ihrer Zweigstelle konfigurieren und dann entsprechend Ihren Sicherheitsanforderungen angeben, welche DNS-Protokolle (DNS-over-Port-53, DoT oder DoH) jeder Standort verwenden kann.

Auswahl des DNS-Protokolls

Wählen Sie das passende DNS-Protokoll basierend auf Ihren Sicherheits- und Kompatibilitätsanforderungen aus:

- DNS-over-Port-53 (Do53) — Verwenden Sie es für maximale Kompatibilität mit der vorhandenen Netzwerkinfrastruktur
- DNS-over-TLS (DoT) — Wird verwendet, wenn Sie verschlüsseltes DNS mit dedizierter Porttrennung für die Netzwerküberwachung benötigen
- DNS-over-HTTPS (DoH) — Verwenden Sie diese Option, wenn Sie Netzwerkeinschränkungen umgehen müssen, da der Datenverkehr als reguläres HTTPS angezeigt wird

DNS-Auflösung mit geteiltem Datenverkehr

Route 53 Global Resolver ermöglicht es Unternehmen, sowohl private als auch öffentliche Domains von jedem Standort aus nahtlos aufzulösen, sodass keine komplexen VPN-Konfigurationen oder regionsspezifische DNS-Einstellungen erforderlich sind.

Hybride DNS-Auflösung

Die hybride DNS-Auflösung ermöglicht es Route 53 Global Resolver, Anfragen von lokalen Benutzern und Anwendungen an private Anwendungen gleichzeitig zu lösen. AWS

Globaler Zugriff auf private Zonen

Der globale Zugriff auf private Zonen erweitert die Reichweite der privaten gehosteten Zonen von Amazon Route 53 über die VPC-Grenzen hinaus. Autorisierte Kunden überall im Internet können private Domainnamen auflösen, sodass verteilte Teams ohne herkömmliche Anforderungen an die Netzwerkkonnektivität auf interne Ressourcen zugreifen können.

Reibungsloser Failover

Ein nahtloses Failover gewährleistet den kontinuierlichen Zugriff auf private und öffentliche Ressourcen, auch wenn einzelne AWS Regionen nicht verfügbar sind. Die Anycast-Architektur

leitet Abfragen automatisch an fehlerfreie Regionen weiter und sorgt gleichzeitig für ein konsistentes Auflösungsverhalten.

Hohe Verfügbarkeit und globale Präsenz

Route 53 Global Resolver bietet Verfügbarkeit auf Unternehmensniveau durch eine verteilte Architektur und automatische Failover-Funktionen.

Einsatz in mehreren Regionen

Bei der Bereitstellung in mehreren Regionen werden Route 53 Global Resolver-Instanzen auf mindestens 2 AWS Regionen verteilt, um eine hohe Verfügbarkeit zu gewährleisten und ein Failover bei Serviceausfällen zu ermöglichen. Sie können je nach Ihren geografischen Anforderungen und Compliance-Anforderungen bestimmte Regionen auswählen.

Automatische geografische Optimierung

Die automatische geografische Optimierung leitet DNS-Abfragen basierend auf Netzwerktopologie und Latenz an die nächstgelegene verfügbare AWS Region weiter. Dies reduziert die Reaktionszeiten und verbessert die Benutzererfahrung für global verteilte Unternehmen.

Integrierte Redundanz

Die integrierte Redundanz gewährleistet die Servicekontinuität durch automatischen Failover auf alternative Regionen, wenn primäre Regionen nicht mehr verfügbar sind. Die Clients verwenden weiterhin dieselben Anycast-IP-Adressen, während der Datenverkehr transparent umgeleitet wird.

DNS-Auflösung und Weiterleitung

Auflösung einer privaten gehosteten Zone

Die Auflösung privat gehosteter Zonen ermöglicht es Route 53 Global Resolver, DNS-Abfragen für private gehostete Route 53 53-Zonen in allen AWS Regionen aufzulösen. Auf diese Weise können autorisierte Clients Domänen für Anwendungen und Ressourcen, die von Route 53 gehostet werden, von überall im Internet aus auflösen.

DNS mit geteiltem Horizont

Split-Horizon DNS bietet je nach Client, der die Anfrage stellt, unterschiedliche DNS-Antworten. Route 53 Global Resolver kann öffentliche Domänen im Internet auflösen und gleichzeitig private Domänen auflösen und bietet so einen nahtlosen Zugriff auf öffentliche und private Ressourcen.

DNSSEC-Validierung

Die DNSSEC-Validierung verifiziert die Authentizität und Integrität von DNS-Antworten von öffentlichen Nameservern für mit DNSSEC signierte Domains. Diese Validierung stellt sicher, dass DNS-Antworten während der Übertragung nicht manipuliert wurden, und bietet so Schutz vor DNS-Spoofing- und Cache-Poisoning-Angriffen.

DNS-Client-Subnetz (ECS)

Das EDNS-Client-Subnetz ist eine optionale Funktion, die Client-Subnetzinformationen in DNS-Abfragen an autoritative Nameserver weiterleitet. Dies ermöglicht genauere geografisch basierte DNS-Antworten und reduziert möglicherweise die Latenz, indem Clients zu Netzwerken oder Servern weitergeleitet werden, die sich näher befinden. Für DNS-over-TLS (DoT) - und DNS-over-HTTPS (DoH) -Verbindungen können Sie EDNS0 verwenden, um die Client-IP-Adressinformationen zu übergeben. Wenn ECS auf Global Resolver aktiviert ist, fügt der Dienst automatisch die Client-IP ein, sofern sie nicht in der Abfrage angegeben ist.

DNS-Filterung und Domänenlisten

Route 53 Global Resolver bietet domänenbasierte Filterung mithilfe von Domänenlisten, die von verwaltet werden AWS , um bestimmte Domänen zu blockieren oder zuzulassen.

Regeln für die DNS-Filterung

DNS-Filterregeln definieren, wie Route 53 Global Resolver DNS-Abfragen auf der Grundlage von Domänenübereinstimmungskriterien verarbeitet. Regeln werden in der Reihenfolge ihrer Priorität ausgewertet und können Aktionen (ALLOW, BLOCK oder ALERT) für Abfragen an bestimmte Domänen oder Domänenkategorien angeben.

Domänenlisten

Domänenlisten sind Sammlungen von Domänen, die in Filterregeln verwendet werden. Sie können sein:

- Benutzerdefinierte Domainlisten — Domainsammlungen, die Sie erstellen und verwalten
- AWS verwaltete Domainlisten — Vorkonfigurierte Bedrohungslisten und Inhaltskategorien AWS , die mithilfe von Bedrohungsinformationen bösartige Domänen identifizieren. Zu den verfügbaren Bedrohungslisten gehören:
  - Malware-Domänen — Domänen, von denen bekannt ist, dass sie Malware hosten oder verteilen

- Steuerung und Kontrolle von Botnetzen — Domänen, die von Botnetzen für die Befehls- und Kontrollkommunikation verwendet werden
- Spam — Domains, die mit Spam und unerwünschten E-Mail-Kampagnen in Verbindung stehen
- Phishing — Domains, die bei Phishing-Angriffen verwendet werden, um Anmeldeinformationen und persönliche Daten zu stehlen
- GuardDuty Amazon-Bedrohungsliste — Domänen, die durch GuardDuty Threat Intelligence identifiziert wurden

Zu den verfügbaren Inhaltskategorien gehören soziale Medien, Glücksspiel und andere Kategorien, mit denen Unternehmen den Zugriff auf bestimmte Arten von Inhalten kontrollieren können.

Einzelne Domainspezifikationen in verwalteten Listen können nicht angezeigt oder bearbeitet werden, um geistiges Eigentum zu schützen und die Wirksamkeit der Sicherheit zu gewährleisten.

Erweiterte Erkennung von DNS-Bedrohungen

Route 53 Global Resolver verwendet dynamische algorithmische Analysen, um fortgeschrittene DNS-Bedrohungen wie DNS-Tunneling und Algorithmen zur Domaingenerierung zu erkennen. Im Gegensatz zu Domainlisten, die mit bekannten schädlichen Domains übereinstimmen, analysiert die algorithmische Erkennung DNS-Abfragemuster in Echtzeit, um verdächtiges Verhalten zu identifizieren.

Erkennung von DNS-Tunneling

DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.

Erkennung durch einen Algorithmus zur Domänengenerierung (DGA)

Algorithmen zur Domaingenerierung (DGAs) werden von Angreifern verwendet, um eine große Anzahl von Domainnamen für ihre command-and-control Server zu erstellen.

Schwellenwerte für das Vertrauen

Jeder Erkennungsalgorithmus gibt einen Konfidenzwert aus, der die Regelauslösung bestimmt. Höhere Vertrauensschwellen reduzieren Fehlalarme, können aber ausgeklügelte Angriffe

übersehen. Niedrigere Schwellenwerte erhöhen die Erkennungsempfindlichkeit, erfordern jedoch zusätzliche Alarmanalysen, um falsch positive Ergebnisse herauszufiltern.

Einschränkungen der Aktionen

Nur Support `ALERT` und `BLOCK` Aktionen für erweiterte Regeln zum Schutz vor Bedrohungen. Die `ALLOW` Aktion wird nicht unterstützt, da die algorithmische Erkennung harmlosen Datenverkehr nicht eindeutig klassifizieren kann, sondern nur potenziell bösartige Muster identifizieren kann.

Überwachung und Protokollierung

-Protokolle abfragen

Abfrageprotokolle enthalten detaillierte Informationen zu DNS-Abfragen, die von Route 53 Global Resolver verarbeitet werden, einschließlich Quell-IP, abgefragter Domain, Antwortcode, ergriffenen Richtlinienaktionen und Zeitstempel. Protokolle können zur Analyse und zur Erstellung von Compliance-Berichten an Amazon CloudWatch, Amazon Data Firehose oder Amazon Simple Storage Service übermittelt werden.

OCSF-Format

Das Open Cybersecurity Schema Framework (OCSF) -Format ist ein standardisiertes Protokollierungsformat, das von Route 53 Global Resolver für DNS-Abfrageprotokolle verwendet wird. Dieses Format bietet konsistente, strukturierte Daten, die sich problemlos in SIEM-Systeme (Security Information and Event Management) und andere Sicherheitstools integrieren lassen.

Ziele protokollieren

Protokollziele bestimmen, wohin DNS-Abfrageprotokolle übermittelt werden, wobei jedes Protokoll unterschiedliche Merkmale aufweist:

- Amazon Simple Storage Service — Kostengünstige Langzeitlagerung, ideal für Konformitäts- und Chargenanalysen. Lässt sich in Analysetools wie Amazon Athena und Amazon EMR integrieren.
- Amazon CloudWatch Logs — Überwachung und Alarmierung in Echtzeit mit Integration in CloudWatch Amazon-Alarme und -Dashboards. Unterstützt Log-Insights für Ad-hoc-Abfragen.
- Amazon Data Firehose — Echtzeit-Streaming zu externen Systemen mit integrierten Datentransformationsfunktionen. Unterstützt automatische Skalierung und Pufferung.

Region „Beobachtbarkeit“

Die Observability-Region bestimmt, wohin DNS-Abfrageprotokolle übermittelt werden.

So funktioniert Route 53 Global Resolver

Route 53 Global Resolver ermöglicht eine geteilte DNS-Auflösung zwischen öffentlichen und privaten Domänen, bietet Hochverfügbarkeit über die beiden oder mehr von AWS-Regionen Ihnen ausgewählten Domänen und schützt DNS-Abfragen, indem Anfragen abgefangen und DNS-Filterrichtlinien angewendet werden. Wenn Sie diesen Prozess verstehen, können Sie Probleme beheben und Ihre Implementierung im Hinblick auf Leistung, Verfügbarkeit und Sicherheit optimieren.

Was passiert, wenn Clients DNS-Abfragen stellen

Wenn jemand an Ihrem Standort versucht, eine Domain abzufragen, verarbeitet Route 53 Global Resolver seine DNS-Anfrage über mehrere Sicherheitsebenen.

Die Verarbeitung der DNS-Abfrage umfasst die folgenden aufeinanderfolgenden Schritte:

1. Empfang von Abfragen — Client-Geräte senden DNS-Abfragen an die Anycast-IP-Adressen von Route 53 Global Resolver. Das Anycast-Routing leitet Anfragen automatisch an die nächstgelegene Region weiter. AWS
2. Authentifizierung — Route 53 Global Resolver authentifiziert den Client mithilfe konfigurierter Authentifizierungsmethoden (tokenbasiert für DoH/DoT oder IP-Zugriffsquelle für alle Protokolle).
3. Richtlinienbewertung — Der Dienst bewertet DNS-Abfragen anhand konfigurierter Sicherheitsrichtlinien und Domänenlisten, um die geeignete Aktion (Zulassen, Blockieren oder Alarmen) zu ermitteln. Bei Abfragen, die auf privat gehostete Zonen abzielen, überprüft Route 53 Global Resolver, ob der Client auf der Grundlage der von Ihrem Administrator verwalteten DNS-View-Regel für den Zugriff auf die private Domain autorisiert ist, bevor er mit der Lösung fortfährt.
4. Lösung — Bei zulässigen Abfragen führt Route 53 Global Resolver die DNS-Auflösung je nach Bedarf mit öffentlichen DNS-Resolvern oder privaten Hosting-Zonenauflösungen durch.
5. Antwortzustellung — Der Dienst sendet die DNS-Antwort an den Client zurück und protokolliert die Abfragedetails zur Überwachung und Analyse.

Globale Anycast-Architektur

Route 53 Global Resolver verwendet Anycast-IP-Adressen, um globale Verfügbarkeit und automatisches geografisches Routing zu gewährleisten.

Route 53 Global Resolver verwendet Anycast-IP-Adressen, um Folgendes bereitzustellen:

- Automatisches geografisches Routing — DNS-Abfragen werden automatisch an die nächstgelegene AWS Region weitergeleitet, um eine optimale Leistung zu erzielen.
- Integrierte Redundanz — Wenn eine Region nicht verfügbar ist, wird der Datenverkehr automatisch auf die nächstgelegene Region umgeleitet.
- Konsistente IP-Adressen — Clients verwenden unabhängig von ihrem Standort dieselben Anycast-IP-Adressen, was die Konfiguration vereinfacht.

DNS-Filterung und Sicherheit

Route 53 Global Resolver bietet umfassende DNS-Filterung und Sicherheit über mehrere Ebenen. Das Diagramm zur DNS-Filterung und Sicherheitsarchitektur zeigt, wie Abfragen über Authentifizierungs-, Richtlinienbewertungs- und Auflösungsebenen verarbeitet werden.

Route 53 Global Resolver bietet umfassende DNS-Sicherheit durch:

- Domainbasierte Filterung — Blockieren oder Zulassen von Abfragen, die auf Domainnamen basieren, mithilfe benutzerdefinierter oder AWS verwalteter Domainlisten.
- Integration von Bedrohungsinformationen — Nutzen Sie AWS verwaltete Bedrohungsinformationen, um bekannte bösartige Domänen automatisch zu blockieren.
- Erweiterte Bedrohungserkennung — Erkennen und blockieren Sie DNS-Tunnelversuche und DGA-Muster (Domain Generation Algorithm).
- Überwachung in Echtzeit — Generieren Sie Warnmeldungen und Protokolle für Sicherheitsereignisse und Richtlinienverstöße.

DNS-Sicherheit und Split-Horizon-Anwendungsfälle für Route 53 Global Resolver

Route 53 Global Resolver adressiert drei primäre DNS-Herausforderungen für Unternehmen:

Ermöglicht die Aufteilung des Datenverkehrs zwischen öffentlicher und privater DNS-Auflösung

Ermöglichen Sie den globalen Zugriff auf private gehostete Zonen (PHZs) auf Amazon Route 53 von jedem beliebigen Standort aus und lösen Sie gleichzeitig öffentliche Domänen im Internet auf. Ermöglichen Sie es entfernten Standorten und Zweigstellen, interne Anwendungsnamen ohne komplexe VPN-Konfigurationen oder regionsspezifische Weiterleitungen aufzulösen.

Implementieren Sie Split-Horizon-DNS, um je nach dem Client, der die Anfrage stellt, unterschiedliche DNS-Antworten bereitzustellen und so Remote-Clients bei der Lösung von Anfragen für private und öffentliche Domänen zu unterstützen.

Schutz des DNS-Datenverkehrs vor DNS-Exfiltrationsangriffen

Schützen Sie entfernte Standorte und Zweigstellen vor DNS-basierten Datenexfiltrationsangriffen, indem Sie Anfragen an bösartige Domänen filtern. Verbessern Sie den Datenschutz, indem Sie den DNS-Verkehr während der Übertragung mit DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT) verschlüsseln, um sicherzustellen, dass nur autorisierte Kunden auf Ihre DNS-Dienste zugreifen können. Wenden Sie Sicherheitsrichtlinien an, um Bedrohungen wie DNS-Tunneling und Algorithmen zur Domaingenerierung zu blockieren (). DGAs Überprüfen Sie die Authentizität von DNS-Antworten mithilfe von DNSSEC (Domain Name System Security Extensions) für mit DNSSEC signierte Domänen, um sich vor DNS-Spoofing- und Cache-Poisoning-Angriffen zu schützen.

Hohe Verfügbarkeit und globale Präsenz

Erzielen Sie eine hohe Verfügbarkeit durch globale Bereitstellung und sorgen Sie über eine einzige Verwaltungsoberfläche für eine weltweit einheitliche DNS-Konfiguration. Route 53 Global Resolver läuft über das von AWS-Regionen Ihnen gewählte System und verwendet Anycast-IP-Adressen, die Abfragen automatisch an die nächstgelegene verfügbare Region weiterleiten, um optimale Leistung und Zuverlässigkeit zu gewährleisten. Weltweit tätige Unternehmen können DNS-Richtlinien zentral konfigurieren und verwalten und gleichzeitig ihren Kunden einen einzigen Satz von IP-Adressen zur Verfügung stellen, die global funktionieren und die automatische geografische Optimierung ermöglichen. Die integrierte Redundanz gewährleistet die Servicekontinuität, auch wenn einzelne Regionen nicht mehr verfügbar sind.

Zusätzliche Funktionen unterstützen die folgenden Hauptanwendungsfälle:

Implementierung von DNS-Filter- und Inhaltsrichtlinien

Steuern Sie den Internetzugang an mehreren Standorten, indem Sie benutzerdefinierte Domainlisten erstellen oder AWS verwaltete Domainlisten verwenden. Um Sie bei der Implementierung von Filter- und Inhaltsrichtlinien entsprechend Ihren Anforderungen zu unterstützen, enthalten verwaltete Domainlisten mehrere Kategorien von DNS-Bedrohungen, die mehrere Domänen abdecken. Konfigurieren Sie die Zugriffsquelle mithilfe von IP-Zulassungslisten oder Zugriffstoken und richten Sie unterschiedliche Filterrichtlinien für verschiedene Bürostandorte oder Kundengruppen ein.

Flexible Authentifizierung für verschiedene Bereitstellungsszenarien

Wählen Sie die Authentifizierungsmethode, die für Ihre Bereitstellung am besten geeignet ist: tokenbasierte Authentifizierung oder IP-basierte Authentifizierung mithilfe der Zulassungslisten für den CIDR-Quellbereich.

Wahrung von Transparenz und Einhaltung von Vorschriften

Überwachen Sie die DNS-Aktivitäten in Ihrer gesamten Organisation, indem Sie Protokolle an Amazon CloudWatch, Firehose oder Amazon Simple Storage Service senden. Wählen Sie eine einzige Zielregion für die zentrale Speicherung von Protokollen, um Sicherheitsüberprüfungen, Compliance-Anforderungen und Bedrohungsuntersuchungen zu unterstützen.

AWS Dienste, die für verbesserte DNS-Sicherheit in Route 53 Global Resolver integriert sind

Route 53 Global Resolver lässt sich nahtlos in andere AWS Dienste integrieren und bietet umfassende DNS-Sicherheits- und Verwaltungsfunktionen. Diese Integrationen erweitern die Kernfunktionen von Route 53 Global Resolver und ermöglichen erweiterte Anwendungsfälle:

Amazon Route 53

Route 53 Global Resolver ist in Amazon Route 53 integriert, um private Hosting-Zonen weltweit aufzulösen. Weitere Informationen finden Sie im Amazon Route 53-Entwicklerhandbuch.

Amazon CloudWatch

Route 53 Global Resolver kann Abfrageprotokolle CloudWatch zur Überwachung und Analyse an Amazon senden. Weitere Informationen finden Sie im CloudWatchAmazon-Benutzerhandbuch.

Amazon Simple Storage Service

Route 53 Global Resolver kann Abfrageprotokolle zur langfristigen Speicherung und Analyse in Amazon Simple Storage Service-Buckets speichern. Weitere Informationen finden Sie im Amazon S3 S3-Benutzerhandbuch.

Amazon Data Firehose

Route 53 Global Resolver kann Abfrageprotokolle zur Echtzeitverarbeitung an Amazon Data Firehose streamen. Weitere Informationen finden Sie im Amazon Data Firehose Developer Guide.

Route 53 Resolver DNS Firewall

Route 53 Global Resolver ergänzt die Route 53 Resolver DNS Firewall durch globale DNS-Filterfunktionen. Weitere Informationen finden Sie in der Dokumentation zur Route 53 Resolver DNS Firewall.

AWS Global Accelerator

Route 53 Global Resolver arbeitet mit AWS Global Accelerator , um eine optimierte globale Netzwerkleistung für die DNS-Auflösung bereitzustellen. Weitere Informationen finden Sie im AWS Global Accelerator -Entwicklerhandbuch.

So greifen Sie über Schnittstellen auf Route 53 Global Resolver zu und verwalten ihn AWS

Route 53 Global Resolver bietet mehrere Zugriffsmethoden, um unterschiedlichen Verwaltungspräferenzen und Automatisierungsanforderungen gerecht zu werden. Sie können Route 53 Global Resolver über diese Schnittstellen verwalten:

AWS-Managementkonsole

Das AWS-Managementkonsole bietet eine webbasierte Oberfläche für Route 53 Global Resolver. Sie können die Konsole verwenden, um DNS-Filterrichtlinien zu konfigurieren, Authentifizierungseinstellungen zu verwalten und Abfrageprotokolle zu überwachen.

AWS Command Line Interface (AWS CLI)

Das AWS CLI bietet direkten Zugriff auf Route 53 Global Resolver API-Operationen. Sie können den verwenden AWS CLI , um Route 53 Global Resolver-Aufgaben zu automatisieren und sie in Ihre Skripte und Workflows zu integrieren.

AWS SDKs

AWS bietet SDKs für viele Programmiersprachen. Sie können das verwenden SDKs , um die Cloud Resolver-Funktionalität in Ihre Anwendungen zu integrieren.

REST-API

Route 53 Global Resolver bietet eine REST-API, mit der Sie Ihre DNS-Auflösungs- und Filterrichtlinien programmgesteuert verwalten können.

Unterstützt AWS-Regionen

Route 53 Global Resolver ist in den folgenden AWS-Regionen Versionen verfügbar:

- Region USA Ost (Nord-Virginia)
- Region USA Ost (Ohio)
- Region USA West (Nordkalifornien)
- Region USA West (Oregon)
- Region Europa (Frankfurt)
- Region Europa (Irland)
- Region Europa (London)
- Region Asien-Pazifik (Mumbai)
- Region Asien-Pazifik (Singapur)
- Region Asien-Pazifik (Tokio)
- Region Asien-Pazifik (Sydney)

Kontozugriff für Route 53 Global Resolver einrichten

Bevor Sie Route 53 Global Resolver verwenden können, benötigen Sie ein AWS Konto und die entsprechenden Berechtigungen für den Zugriff auf Route 53 Global Resolver-Ressourcen. Dazu gehört das Erstellen von IAM-Benutzern und -Rollen mit den erforderlichen Berechtigungen.

Dieser Abschnitt führt Sie durch die Schritte, die zur Konfiguration von Benutzern und Rollen für den Zugriff auf Route 53 Global Resolver erforderlich sind.

Topics

Melden Sie sich für eine an AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können Ihre aktuellen Kontoaktivitäten jederzeit einsehen und Ihr Konto verwalten, indem Sie zu https://aws.amazon.com/gehen und Mein Konto auswählen.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Richtlinien und Rollen erstellen

Konfigurieren Sie AWS Identity and Access Management (IAM) -Berechtigungen, damit Ihr Team Route 53 Global Resolver-Ressourcen bereitstellen und verwalten kann. Sie können Administratorberechtigungen für vollen Zugriff oder Leseberechtigungen für die Überwachung und Anzeige von Konfigurationen verwenden.

Für alle Route 53 Global Resolver API-Operationen sind entsprechende IAM-Berechtigungen erforderlich. Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, geben API-Aufrufe (401) - oder `AccessDeniedException` `UnauthorizedException` (401) Fehler zurück.

Administrative Berechtigungen

Wenn Sie Route 53 Global Resolver zum ersten Mal einrichten oder alle Aspekte des Dienstes verwalten, benötigen Sie Administratorrechte. Sie können diese AWS verwalteten Richtlinien verwenden:

- `AmazonRoute53GlobalResolverFullAccess`- Bietet vollen Zugriff auf Route 53 Global Resolver-Ressourcen, einschließlich Erstellung, Aktualisierung und Löschung globaler Resolver, DNS-Ansichten, Firewallregeln und Domänenlisten
- `AmazonRoute53FullAccess`- Erforderlich, wenn Sie die private gehostete Zonenweiterleitung verwenden möchten
- `CloudWatchLogsFullAccess`- Erforderlich, wenn Sie Logs an Amazon senden möchten CloudWatch
- `AmazonS3FullAccess`- Erforderlich, wenn Sie Firewall-Domänenlisten aus Amazon S3 importieren oder Protokolle an Amazon S3 senden möchten

Schreibgeschützte Berechtigungen

Wenn Sie nur die Konfigurationen und Protokolle von Route 53 Global Resolver anzeigen müssen, können Sie diese AWS verwalteten Richtlinien verwenden:

- `AmazonRoute53GlobalResolverReadOnlyAccess`- Bietet schreibgeschützten Zugriff auf Route 53 Global Resolver-Ressourcen, einschließlich der Anzeige globaler Resolver, DNS-Ansichten, Firewallregeln, Domänenlisten und Zugriffsquellen
- `AmazonRoute53ReadOnlyAccess`- Erforderlich, um private gehostete Zonenzuordnungen anzuzeigen
- `CloudWatchReadOnlyAccess`- Erforderlich, um Protokolle in Amazon anzuzeigen CloudWatch
- `AmazonS3ReadOnlyAccess`- Erforderlich, um in Amazon S3 gespeicherte Firewall-Domänenlistendateien anzuzeigen

Überlegungen zu Netzwerken

Beachten Sie vor der Implementierung von Route 53 Global Resolver die folgenden Netzwerkanforderungen:

IP-Bereiche der Clients

Dies ist nur erforderlich, wenn die Authentifizierung auf Basis der Zugriffsquelle verwendet wird. Identifizieren Sie die IP-Adressbereiche (CIDR-Blöcke) für alle Clients, die Route 53 Global Resolver verwenden werden. Sie benötigen diese für die Konfiguration der Regeln für Ihre Zugriffsquelle.

DNS-Protokolle

Ermitteln Sie, welche DNS-Protokolle Ihre Clients verwenden werden:

- Do53 — Standard-DNS über Port 53 (UDP/TCP)
- DoH — für verschlüsselte Abfragen DNS-over-HTTPS
- DoT - DNS-over-TLS für verschlüsselte Abfragen

Firewall und Sicherheitsgruppen

Stellen Sie sicher, dass Ihre Netzwerk-Firewalls und Sicherheitsgruppen ausgehenden Datenverkehr zu Route 53 Global Resolver Anycast-IP-Adressen an den entsprechenden Ports zulassen (53 für Do53, 443 für DoH, 853 für DoT).

Tutorial: Erstellen Sie Ihren ersten Route 53 Global Resolver

In diesem Handbuch für die ersten Schritte werden die grundlegenden Komponenten von Route 53 Global Resolver und optional die Erstellung einer einfachen DNS-Filterung demonstriert. Dieses Tutorial behandelt die Kernkonzepte, beinhaltet jedoch keine Produktionsanforderungen wie Client-Konfiguration, Protokollierung oder Auflösung privater Domänen.

Wenn Sie fertig sind, verfügen Sie über ein grundlegendes Route 53 Global Resolver-Setup, das DNS-Abfragen filtern und bösartige Domains blockieren kann.

In den folgenden Abschnitten wird beschrieben, wie Sie schnell mit der DNS-Sicherheit und Filterung mithilfe von Route 53 Global Resolver beginnen können.

Voraussetzungen

Bevor Sie Route 53 Global Resolver verwenden können, benötigen Sie ein AWS Konto und die entsprechenden Berechtigungen, um auf Route 53 Global Resolver-Komponenten zuzugreifen, diese anzuzeigen und zu bearbeiten. Ihr Systemadministrator muss die unter aufgeführten Schritte ausführen und the section called “Kontozugriff einrichten” dann zu diesem Tutorial zurückkehren.

Schritt 1: Erstellen Sie einen globalen Resolver

Erstellen Sie zunächst eine globale Resolver-Instanz und wählen Sie die AWS Regionen aus, in denen sie betrieben werden soll.

1. Öffnen Sie die Route 53 Global Resolver-Konsole unter https://console.aws.amazon.com/route53globalresolver/.
2. Wählen Sie Create Global Resolver aus.
3. Geben Sie unter Name einen aussagekräftigen Namen für Ihren globalen Resolver ein.
4. Geben Sie unter Beschreibung optional eine Beschreibung ein.
5. Wählen Sie unter Regionen zwei oder mehr Regionen aus, AWS-Regionen in denen Sie den globalen Resolver instanziieren möchten. Wählen Sie Regionen aus, die Ihren Kunden am nächsten liegen, um eine optimale Leistung zu erzielen.
6. Fügen Sie optional Tags hinzu, um Ihre Ressourcen besser organisieren und verwalten zu können.
7. Wählen Sie Create Global Resolver aus.

Sie erhalten sofort IPv4 Anycast-Adressen, über die Ihre Kunden den Resolver erreichen können. Der Prozess zur Erstellung des globalen Resolvers dauert einige Minuten, bis die Adressen funktionsfähig sind.

Schritt 2: Erstellen Sie eine DNS-Ansicht und konfigurieren Sie die Authentifizierung

Erstellen Sie eine DNS-Ansicht, um Ihre Clients zu organisieren und die Authentifizierung mithilfe von IP-Zugriffsquellen zu konfigurieren. In diesem Tutorial wird die IP-basierte Authentifizierung verwendet. Sie können auch Zugriffstoken für DoH/DOT-Protokolle verwenden.

1. Wählen Sie in der Route 53 Global Resolver-Konsole Ihren globalen Resolver aus.

2. Wählen Sie DNS-Ansicht erstellen aus.
3. Geben Sie unter Name einen beschreibenden Namen für Ihre DNS-Ansicht ein.
4. Geben Sie unter Beschreibung optional eine Beschreibung ein.
5. Wählen Sie DNS-Ansicht erstellen aus.
6. Nachdem die DNS-Ansicht erstellt wurde, wählen Sie Zugriffsquelle und dann Zugriffsquelle erstellen aus.
7. Geben Sie für CIDR-Block den IP-Adressbereich für Ihre Clients ein (z. B.`203.0.113.0/24`).
8. Wählen Sie für Protocol Do53 (DNS over Port 53) für die Grundkonfiguration aus.
9. Wählen Sie Regel für die Zugriffsquelle erstellen aus.

Schritt 3: DNS-Filterregeln konfigurieren (optional)

Richten Sie grundlegende DNS-Filterregeln ein, um den Zugriff auf bösartige Domains zu blockieren.

1. Wählen Sie in Ihrer DNS-Ansicht Firewall-Regeln und dann Firewallregel erstellen aus.
2. Geben Sie unter Name einen beschreibenden Namen für die Regel ein.
3. Geben Sie als Priorität den Wert ein `100` (niedrigere Zahlen haben eine höhere Priorität).
4. Wählen Sie für Aktion die Option Blockieren aus.
5. Wählen Sie als Typ der Domainliste die Option AWS Managed Domain List aus.
6. Wählen Sie unter Liste verwalteter Domänen die Option Malware AmazonGuardDutyThreatListand Botnet Command and Control aus, um bekannte bösartige Domains zu blockieren (Sie können später weitere verwaltete Listen hinzufügen oder benutzerdefinierte Listen erstellen).
7. Wählen Sie Firewallregel erstellen aus.

Schritt 4: Testen Sie Ihre Konfiguration

Testen Sie, ob Ihre Route 53 Global Resolver-Konfiguration ordnungsgemäß funktioniert.

1. Testen Sie die DNS-Auflösung auf einem Client-Computer innerhalb Ihres konfigurierten CIDR-Bereichs mithilfe der Anycast-IP-Adressen, die von Ihrem globalen Resolver bereitgestellt werden:

```
nslookup example.com <anycast-ip-address>
```

2. Stellen Sie sicher, dass legitime Domänen korrekt aufgelöst werden.
3. Testen Sie, ob blockierte Domains ordnungsgemäß gefiltert wurden. Sie können eine benutzerdefinierte Domänenliste mit einer Testdomäne erstellen, um zu überprüfen, ob Ihre Firewallregeln ordnungsgemäß funktionieren. Weitere Informationen zu verwalteten Domänenlisten finden Sie unter Verwaltete Domänenlisten.
4. Suchen Sie in der Route 53 Global Resolver-Konsole nach Abfrageprotokollen und Filteraktivitäten.

Umfassende Testverfahren und Problembehebungen finden Sie unter Problembehandlung bei Route 53 Global Resolver.

Schritt 5: Überwachung der DNS-Aktivität

Konfigurieren Sie die Protokollierung für Ihre DNS-Aktivität.

1. Wählen Sie eine Observability-Region aus.
2. Wählen Sie das Ziel für Abfrage-Logs aus.

Umfassende Testverfahren und Problembehebung finden Sie unter Route 53 Global Resolver testen und beheben.

Schritt 6: Aufräumen (optional)

Wenn Sie diese Konfiguration zu Testzwecken erstellt haben und Route 53 Global Resolver nicht weiter verwenden möchten, bereinigen Sie die Ressourcen, um laufende Gebühren zu vermeiden.

1. Löschen Sie in der Route 53 Global Resolver-Konsole alle Firewallregeln, die Sie erstellt haben.
2. Löschen Sie alle Access Source-Regeln, die Sie erstellt haben.
3. Löschen Sie die DNS-Ansicht.
4. Löschen Sie den globalen Resolver.

> **Important**
>
> Durch das Löschen dieser Ressourcen wird die DNS-Auflösung für alle Clients beendet, die für deren Verwendung konfiguriert sind. Aktualisieren Sie Ihre Client-Konfigurationen, bevor Sie den Resolver löschen oder die Zugriffsregeln entfernen.

Nächste Schritte

Da Sie nun über eine grundlegende Route 53 Global Resolver-Konfiguration verfügen, können Sie weitere Funktionen erkunden:

- Konfigurieren Sie Client-Geräte so, dass sie Ihren Resolver verwenden (für die Produktion erforderlich). Aktualisieren Sie Ihre Client-DNS-Einstellungen, um die von Ihrem Global Resolver bereitgestellten Anycast-IP-Adressen zu verwenden.
- Richten Sie die Protokollierung zur Überwachung und Einhaltung von Vorschriften ein (für die Produktion empfohlen). Konfigurieren Sie die Protokollierung bei Amazon CloudWatch, Amazon S3 oder Amazon Data Firehose für die Überwachung und Analyse. Weitere Informationen finden Sie unter Überwachung der DNS-Aktivität und -Leistung mit Route 53 Global Resolver.
- Konfigurieren Sie die Weiterleitung von privaten gehosteten Zonen für interne Domains (erforderlich, wenn Sie über private AWS Ressourcen verfügen). Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.
- Richten Sie verschlüsselte DNS-Konnektivität mit DNS-over-HTTPS (DoH) oder DNS-over-TLS (DoT) ein. Weitere Informationen finden Sie unter Verschlüsseltes DNS konfigurieren.
- Erstellen Sie benutzerdefinierte Domain-Listen und erweiterte Filterregeln. Weitere Informationen finden Sie unter DNS-Filterung.

Verwaltung von DNS-Ansichten mit Route 53 Global Resolver

Sie können laufende Route 53 Global Resolver-Operationen verwalten, einschließlich der Aktualisierung von DNS-Ansichten, um zu steuern, welche Client-Gerätegruppen in interne Ressourcen aufgelöst werden können und welche Domänen gefiltert werden sollen.

DNS-Ansichten verwalten

Nachdem Sie DNS-Ansichten erstellt haben, können Sie ihre Konfiguration aktualisieren, sie aktivieren oder deaktivieren und ihren Lebenszyklus verwalten.

DNS-Ansichten für Client-Gerätegruppen erstellen

Eine DNS-Ansicht ist eine logische Gruppierung, die Sicherheitsrichtlinien für eine Gruppe von Client-Geräten definiert, z. B. für Mitarbeiter an entfernten Standorten, Geräte in Zweigstellen oder Geräte vor Ort. Jede Ansicht hat ihre eigenen Authentifizierungsanforderungen, Filterregeln und Zuordnungen zu privaten gehosteten Zonen.

Um eine DNS-Ansicht zu erstellen

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/route53globalresolver/.
2. Wählen Sie Ihren globalen Resolver aus der Liste aus.
3. Wählen Sie den Tab DNS-Ansichten.
4. Wählen Sie DNS-Ansicht erstellen.
5. Gehen Sie im Abschnitt „Details zur DNS-Ansicht“ wie folgt vor:
   a. Geben Sie als DNS-View-Name einen aussagekräftigen Namen für Ihre DNS-Ansicht ein (bis zu 128 Zeichen).
   b. (Optional) Geben Sie unter Beschreibung eine Beschreibung für Ihre DNS-Ansicht ein (bis zu 255 Zeichen).
6. Konfigurieren Sie im Abschnitt zur Verarbeitung von DNS-Abfragen die folgenden Einstellungen:
   - DNSSEC-Validierung — Wählen Sie Aktivieren oder Deaktivieren. Die DNSSEC-Validierung ermöglicht es dem Global Resolver, die Authentizität von DNS-Antworten zu überprüfen.
   - Firewallregeln schlagen beim Öffnen fehl — Wählen Sie Aktivieren, damit Abfragen fortgesetzt werden können, wenn die DNS-Firewall sie nicht auswerten kann, oder Deaktivieren, um solche Abfragen zu blockieren.
   - EDNS0-Client-Subnetz — Wählen Sie „Aktivieren“, um die Genauigkeit der Client-Ortung für die Weiterleitung von Datenverkehr zu Ressourcen in der Nähe und effizientes Caching zu verbessern, oder „Deaktivieren“, um diese Funktion zu deaktivieren.
7. Wählen Sie „DNS-Ansicht erstellen“.

Nachdem Sie die DNS-Ansicht erstellt haben, können Sie Zugriffskontrollen, Firewallregeln und Zuordnungen von privaten gehosteten Zonen konfigurieren.

DNS-Ansichten bearbeiten

Sie können die Einstellungen für die DNS-Ansicht nach der Erstellung ändern, einschließlich der Optionen für die Verarbeitung von DNS-Abfragen und der zugehörigen Ressourcen.

Um eine DNS-Ansicht zu bearbeiten

1. Navigieren Sie in der Konsole zu Ihrem globalen Resolver.
2. Wählen Sie den Tab DNS-Ansichten.
3. Wählen Sie die DNS-Ansicht aus, die Sie bearbeiten möchten, und wählen Sie Bearbeiten.
4. Ändern Sie die Einstellungen für die DNS-Ansicht nach Bedarf und wählen Sie Änderungen speichern.

DNS-Ansichten aktivieren und deaktivieren

Sie können eine DNS-Ansicht vorübergehend deaktivieren, ohne sie zu löschen. Wenn diese Option deaktiviert ist, beendet der globale Resolver die Bearbeitung von Anfragen für Client-Geräte, die mit dieser DNS-Ansicht verknüpft sind.

> **Warning**
>
> Wenn Sie eine DNS-Ansicht deaktivieren, wird die DNS-Auflösung für alle Client-Geräte, die dieser Ansicht zugeordnet sind, sofort beendet. Stellen Sie sicher, dass Sie eine alternative DNS-Auflösung für die betroffenen Client-Geräte konfiguriert haben.

DNS-Ansichten löschen

Bevor Sie eine DNS-Ansicht löschen können, müssen Sie zunächst alle zugehörigen Ressourcen löschen, einschließlich Zugriffsquellenregeln, Zugriffstoken, Firewallregeln und Zuordnungen zu privaten gehosteten Zonen.

> **Warning**
>
> Das Löschen einer DNS-Ansicht ist irreversibel und beendet sofort die DNS-Auflösung für alle mit dieser Ansicht verknüpften Client-Geräte.

Zuordnungen von privaten gehosteten Zonen verwalten

Sie können private gehostete Zonenzuordnungen nach Bedarf anzeigen, aktualisieren und entfernen, um zu kontrollieren, welche Client-Gerätegruppen Zugriff auf interne Ressourcen haben.

Zuordnungen anzeigen

Um alle Zuordnungen von privaten gehosteten Zonen für eine DNS-Ansicht anzuzeigen, navigieren Sie zu Ihrer DNS-Ansicht und suchen Sie im Abschnitt Private gehostete Zonen nach, um alle zugehörigen Zonen mit ihrem Status und ihren Zuordnungsdetails zu sehen.

Verknüpfungen werden aktualisiert

Sie können den Namen einer privaten Hosted-Zone-Zuordnung aktualisieren, indem Sie die Zuordnung auswählen, Bearbeiten wählen, den Zuordnungsnamen aktualisieren und die Änderungen speichern.

Verknüpfungen werden entfernt

Wenn Sie eine private gehostete Zonenzuweisung entfernen, verwendet Route 53 Global Resolver diese Zone nicht mehr, um DNS-Abfragen für die zugehörige DNS-Ansicht aufzulösen.

> **Warning**
>
> Das Entfernen einer privaten Hosting-Zonenzuordnung wirkt sich sofort auf die DNS-Auflösung aus. Abfragen für Domänen in der getrennten Zone werden mithilfe von öffentlichem DNS anstelle der privaten Zoneneinträge gelöst.

Konfigurieren Sie die Einstellungen für DNS-Ansichten in Route 53 Global Resolver

Mit Route 53 Global Resolver können Sie je nach Sicherheitsanforderungen und Zugriffsanforderungen unterschiedliche DNS-Richtlinien und Zugriffskontrollen für verschiedene Gruppen von Client-Geräten konfigurieren. Richten Sie DNS-Richtlinien und Zugriffskontrollen in Route 53 Global Resolver für verschiedene Gruppen von Client-Geräten auf der Grundlage ihrer Sicherheits- und Zugriffsanforderungen ein.

Konfiguration von DNS-Einstellungen für Client-Gruppen

Jede DNS-Ansicht verfügt über mehrere Einstellungen, mit denen gesteuert wird, wie DNS-Abfragen für verschiedene Client-Gerätegruppen verarbeitet und gelöst werden.

DNSSEC-Validierung

Durch die DNSSEC-Validierung wird sichergestellt, dass DNS-Antworten für öffentliche Domänen authentisch sind und nicht manipuliert wurden. Wenn Sie die DNSSEC-Validierung aktivieren, überprüft Route 53 Global Resolver DNSSEC-Signaturen und gibt SERVFAIL für Domänen mit ungültigen Signaturen zurück.

Erwägen Sie, die DNSSEC-Validierung zu aktivieren, wenn:

- Ihr Unternehmen benötigt eine kryptografische Überprüfung von DNS-Antworten
- Sie möchten sich vor DNS-Spoofing- und Cache-Poisoning-Angriffen schützen
- Sie haben Compliance-Anforderungen, die eine DNSSEC-Validierung erfordern

> **Note**
>
> Die DNSSEC-Validierung gilt nur für öffentliche Domains. Private gehostete Zonen verwenden ihre eigenen Authentifizierungsmechanismen.

EDNS-Client-Subnetz (ECS)

Das EDNS-Client-Subnetz enthält Informationen über den Netzwerkstandort des Clients in DNS-Abfragen, die an autorisierende Server gesendet werden. Auf diese Weise können Netzwerke zur Inhaltsbereitstellung und geografisch verteilte Dienste standortgerechte Antworten bereitstellen.

ECS kann Ihnen helfen:

- Holen Sie sich eine bessere Leistung mit geografisch verteilten Diensten
- Verbessern Sie die Genauigkeit der Netzwerkweiterleitung von Inhalten
- Halten Sie regionale Inhaltsbeschränkungen besser ein

Überlegungen zum Datenschutz:

- ECS gibt einen Teil der Client-IP-Informationen an autorisierende Server weiter (maximal /24 für IPv4 und /48 für) IPv6
- Berücksichtigen Sie vor der Aktivierung die Datenschutzanforderungen Ihres Unternehmens

Die Firewall konnte nicht geöffnet werden

Die Einstellung zum Öffnen der Firewall legt fest, was passiert, wenn DNS-Firewallregeln aufgrund von Dienstbeeinträchtigungen oder Konfigurationsproblemen nicht ausgewertet werden können.

Deaktiviert (Standard)

DNS-Abfragen werden blockiert, wenn Firewallregeln nicht ausgewertet werden können. Dies bietet Ihnen maximale Sicherheit, kann jedoch die Verfügbarkeit bei Serviceproblemen beeinträchtigen.

Aktiviert

DNS-Abfragen sind zulässig, wenn Firewallregeln nicht ausgewertet werden können. Dadurch wird der Verfügbarkeit bei Serviceproblemen Vorrang vor der Sicherheit eingeräumt.

Bewährte Methoden für die Organisation von Client-Gerätegruppen

Beachten Sie beim Entwerfen von DNS-Ansichten für verschiedene Client-Gerätegruppen die folgenden bewährten Methoden:

Unternehmensstrategien anzeigen

- Nach Sicherheitsanforderungen getrennt — Erstellen Sie unterschiedliche Ansichten für Client-Geräte mit unterschiedlichen Sicherheitsfreigaben oder Zugriffsebenen
- Nach Standort organisieren — Verwenden Sie separate Ansichten für verschiedene geografische Standorte oder Netzwerksegmente
- Nach Gerätetyp gruppieren — Erstellen Sie spezielle Ansichten für Server, Workstations, mobile Geräte oder IoT-Geräte
- Verwenden Sie aussagekräftige Namen — Wählen Sie Namen, die den Zweck der Ansicht und die Ziel-Client-Geräte eindeutig angeben

Sicherheitsüberlegungen

- Prinzip der geringsten Rechte — Konfigurieren Sie jede Ansicht mit dem Mindestzugriff, der für die Client-Geräte erforderlich ist
- Standardeinstellung verweigern — Beginnen Sie mit restriktiven Firewallregeln und fügen Sie nach Bedarf Ausnahmen hinzu

- Regelmäßige Überprüfung — Überprüfen und aktualisieren Sie regelmäßig die DNS-Ansichtskonfigurationen
- Nutzung überwachen — Verwenden Sie DNS-Abfrageprotokolle, um die Nutzungsmuster von DNS-Views zu überwachen und zu analysieren

Verwaltung von Zugriffskontrollen mit Zugriffsquellen und Tokens in Route 53 Global Resolver

Route 53 Global Resolver bietet zwei Hauptmethoden zur Steuerung des Zugriffs auf Client-Geräte: Zugriffsquellen für die IP-basierte Authentifizierung und Zugriffstoken für die tokenbasierte Authentifizierung. Dieses Kapitel behandelt beide Ansätze und hilft Ihnen dabei, die richtige Authentifizierungsmethode für Ihre Umgebung auszuwählen und umfassende Zugriffskontrollen zu implementieren.

Topics

Grundlegendes zu den Zugriffskontrollmethoden in Route 53 Global Resolver

Route 53 Global Resolver bietet zwei unterschiedliche Authentifizierungsmethoden zur Steuerung des Client-Zugriffs auf Ihre DNS-Infrastruktur. Jede Methode dient unterschiedlichen Anwendungsfällen und Umgebungen.

IP-basierte Zugriffsquellen

Sie konfigurieren Zugriffsquellenregeln, die DNS-Abfragen auf der Grundlage von Client-IP-Adressen zulassen oder verweigern. Diese Methode eignet sich gut für Umgebungen mit vorhersehbaren IP-Bereichen, z. B. Zweigstellen oder VPN-Verbindungen. Zugriffsquellen unterstützen alle DNS-Protokolle (Do53, DoT und DoH) und bieten Netzwerkadministratoren eine einfache Konfiguration.

Token-basierte Authentifizierung

Zugriffstoken bieten eine sichere Authentifizierung für DoH- und DoT-Protokolle mithilfe verschlüsselter, zeitlich begrenzter Anmeldeinformationen. Diese Methode eignet sich für mobile Clients und Umgebungen, in denen sich IP-Adressen häufig ändern. Sie können Token vor Ablauf erneuern und sie bieten durch Verschlüsselung mehr Sicherheit.

Berücksichtigen Sie bei der Auswahl Ihres Authentifizierungsansatzes die folgenden Faktoren:

Auswahl der richtigen Authentifizierungsmethode

Faktor	Auf Quellen zugreifen	Zugriffstoken
Am besten geeignet für	Feste IP-Bereiche, Büronetzwerke, VPN-Benutzer	Mobile Geräte, dynamische IPs Mitarbeiter, die von zu Hause aus arbeiten
Sicherheitsstufe	Netzwerkbasiert, basiert auf IP-Trust	Verschlüsselte Anmeldedaten, zeitlich begrenzt
Komplexität der Verwaltung	Einfache Verwaltung des IP-Bereichs	Lebenszyklus und Verteilung von Tokens
Protokollunterstützung	Do53, DoT, DoH	Nur DoT, DoH

Sie können beide Methoden gleichzeitig verwenden, um mehrschichtige Sicherheit zu schaffen. Verwenden Sie beispielsweise Zugriffsquellen für Büronetzwerke und Token für Mitarbeiter an entfernten Standorten.

Konfiguration von Zugriffsquellen und Zugriffsquellenregeln

Zugriffsquellen steuern den Client-Zugriff auf der Grundlage von IP-Adressen. Sie erstellen Zugriffsquellenregeln, die angeben, welche IP-Bereiche Ihre DNS-Infrastruktur abfragen können und welche Protokolle sie verwenden können.

Regeln für Zugriffsquellen erstellen

Gehen Sie wie folgt vor, um eine Zugriffsquellenregel zu erstellen, die es bestimmten IP-Bereichen ermöglicht, Ihre DNS-Infrastruktur abzufragen.

1. Öffnen Sie die Route 53 Global Resolver-Konsole und navigieren Sie zu Ihrer DNS-Ansicht.
2. Wählen Sie im Abschnitt Zugriffsquelle die Option Zugriffsquellenregel erstellen aus.
3. Geben Sie unter Name einen aussagekräftigen Namen ein, der den Zweck dieser Regel kennzeichnet, z. B. `office-network` oder`vpn-users`.
4. Geben Sie für IP-Adressbereich die IP-Adressen an, die Zugriff haben sollen. Sie können die CIDR-Notation für IP-Bereiche verwenden: `192.168.1.0/24` oder einzelne IP-Adressen:`203.0.113.5/32`.
5. Wählen Sie unter Protokoll die DNS-Protokolle aus, für die diese Regel gilt:
   - Do53 — Standard-DNS über UDP/TCP (Port 53)
   - DoT — DNS über TLS (Port 853)
   - DoH — DNS über HTTPS (Port 443)
6. Wählen Sie Zugriffsquellenregel erstellen aus.

Client-Geräte aus den angegebenen IP-Bereichen können jetzt Ihre DNS-Infrastruktur mithilfe der ausgewählten Protokolle abfragen.

Grundlegendes zur Bewertung und Priorität von Regeln

Route 53 Global Resolver bewertet die Regeln für die Zugriffsquelle, wenn es darum geht, die richtige zu verwendende Ansicht zu ermitteln.

- Regeln werden von den spezifischsten bis hin zu den am wenigsten spezifischen IP-Bereichen verarbeitet, wobei die spezifischste Übereinstimmungsregel Vorrang hat.
- Wenn keine Regeln übereinstimmen, wird die Anfrage standardmäßig abgelehnt.

Testen Sie Ihre Konfiguration der Zugriffsquelle, indem Sie Abfragen von verschiedenen IP-Adressen aus durchführen, um sicherzustellen, dass die Regeln erwartungsgemäß funktionieren.

Verwaltung von Zugriffstoken für die verschlüsselte Authentifizierung

Zugriffstoken ermöglichen eine verschlüsselte Authentifizierung für DoH- und DoT-Protokolle. Im Gegensatz zu IP-basierten Zugriffsquellen funktionieren Token unabhängig vom Standort des Kunden und bieten durch Verschlüsselungs- und Ablaufkontrollen mehr Sicherheit.

Zugriffstoken erstellen

Gehen Sie wie folgt vor, um Zugriffstoken zur Authentifizierung von Client-Geräten zu erstellen, die DoH- oder DoT-Protokolle verwenden.

1. Öffnen Sie die Route 53 Global Resolver-Konsole und navigieren Sie zu Ihrer DNS-Ansicht.
2. Wählen Sie im Abschnitt Zugriffsquelle die Option Zugriffstoken erstellen aus.
3. Geben Sie unter Name einen aussagekräftigen Namen ein, der den Zweck des Tokens identifiziert, z. B. `mobile-devices` oder`remote-workers-q4`.
4. Geben Sie unter Ablauf an, wann das Token ablaufen soll. Aus Sicherheitsgründen empfehlen wir 90 Tage oder weniger. Berücksichtigen Sie bei der Festlegung des Ablaufzeitraums Ihre Möglichkeiten zur Verteilung und Verlängerung von Tokens.
5. Wählen Sie Zugriffstoken erstellen aus.
6. Verteilen Sie das Token sicher über die sicheren Kommunikationskanäle Ihres Unternehmens an Ihre Client-Geräte.

Konfiguration von Client-Geräten mit Zugriffstoken

Konfigurieren Sie Client-Geräte so, dass sie Zugriffstoken für die Authentifizierung mit Ihrer Route 53 Global Resolver-Infrastruktur verwenden.

DoH-Konfiguration

Um DoH mit Zugriffstoken zu konfigurieren, benötigen Sie den DNS-Namen oder die IP-Adressen Ihres globalen Resolvers:

1. Verwenden Sie die GetGlobalResolver API, um Verbindungsdetails für Ihren Resolver abzurufen.
2. Beachten Sie die `ipv4Addresses` (z. B. 3.3.3.3, 3.3.3.4) und (zum Beispiel `dnsName` a1bc234567890a.route53globalresolver.global.on.aws).
3. Fügen Sie das Token unter Verwendung des DNS-Namens als URL-Parameter in den DoH-Endpunkt ein:

```
https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<token-value>
```

`<token-value>`Ersetzen Sie es durch das tatsächliche Token, das Sie generiert haben.

DoT-Konfiguration

Fügen Sie bei DoT-Abfragen mit Zugriffstoken das Token in eine EDNS0-Option mit den folgenden Spezifikationen ein:

- Optionscode: `0xffa0`
- Optionsdaten: Das Zugriffstoken im Zeichenkettenformat

Die spezifische Implementierung hängt von Ihrer DoT-Client-Software und davon ab, wie sie mit EDNS0-Optionen umgeht.

Verwaltung des Token-Lebenszyklus

Verwalten Sie den Ablauf und die Verlängerung von Tokens, um einen sicheren Zugriff für Ihre Client-Geräte zu gewährleisten.

- Ablaufdaten überwachen — Verfolgen Sie die Ablaufdaten von Tokens und planen Sie Verlängerungen im Voraus.
- Vor Ablauf verlängern — Erstellen Sie neue Token, bevor alte ablaufen, um Serviceunterbrechungen zu vermeiden.
- Wechseln Sie die Tokens regelmäßig — Tauschen Sie Token aus Sicherheitsgründen regelmäßig aus, noch bevor sie ablaufen.
- Widerrufen kompromittierter Token — Löschen Sie Token sofort, wenn Sie vermuten, dass sie kompromittiert wurden.

Erwägen Sie die Implementierung automatisierter Prozesse zur Token-Erneuerung für große Bereitstellungen, um den Verwaltungsaufwand zu reduzieren.

Beispiele für die Plattformkonfiguration

Verwenden Sie diese plattformspezifischen Beispiele, um Client-Geräte mit Ihren Route 53 Global Resolver-Zugriffstoken und Verbindungsdetails zu konfigurieren.

Windows-Konfiguration

Gehen Sie wie folgt vor, um Windows-Clients mithilfe des Befehls netsh für die Verwendung von DoH mit Zugriffstoken zu konfigurieren.

1. Öffnen Sie die Eingabeaufforderung als Administrator.

2. Aktivieren Sie die globale DoH-Einstellung:

```
netsh dns add global doh=yes
```

3. Registrieren Sie DoH-Server mit Zugriffstoken. Ersetzen Sie die Beispielwerte durch Ihre tatsächlichen Resolver-Details:

```
netsh dns add encryption server=3.3.3.3 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
netsh dns add encryption server=3.3.3.4 dohtemplate=https://
a1bc234567890a.route53globalresolver.global.on.aws/dns-query?token=<your-token>
 autoupgrade=yes
```

4. Leeren Sie den DNS-Cache:

```
ipconfig /flushdns
```

5. Überprüfen Sie die Konfiguration:

```
netsh dns show global
```

macOS-Konfiguration

Gehen Sie wie folgt vor, um macOS-Clients mithilfe eines mobilen Konfigurationsprofils für DoH mit Zugriffstoken zu konfigurieren.

Erstellen Sie ein mobiles Konfigurationsprofil mit der folgenden Struktur:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>DNSSettings</key>
      <dict>
        <key>DNSProtocol</key>
        <string>HTTPS</string>
```

```
        <key>ServerAddresses</key>
        <array>
          <string>3.3.3.3</string>
          <string>3.3.3.4</string>
        </array>
        <key>ServerURL</key>
        <string>https://a1bc234567890a.route53globalresolver.global.on.aws/dns-query?
token=<your-token></string>
      </dict>
      <key>PayloadType</key>
      <string>com.apple.dnsSettings.managed</string>
    </dict>
  </array>
</dict>
</plist>
```

Installieren Sie das Profil über Systemeinstellungen > Geräteverwaltung.

Bewährte Methoden und Sicherheitsüberlegungen für die Zugriffskontrolle

Befolgen Sie diese bewährten Methoden, um sichere und effektive Zugriffskontrollen für Ihre Route 53 Global Resolver-Infrastruktur aufrechtzuerhalten.

Bewährte Methoden für die Gewährleistung der Sicherheit

Implementieren Sie diese Sicherheitsmaßnahmen, um Ihre DNS-Infrastruktur zu schützen:

- Verwenden Sie mehrschichtige Authentifizierung — Kombinieren Sie Zugriffsquellen für vertrauenswürdige Netzwerke mit Tokens für mobile Benutzer. Dieser Ansatz bietet umfassenden Schutz und ist für unterschiedliche Kundenszenarien geeignet.
- Implementieren Sie den Zugriff mit den geringsten Rechten — Gewähren Sie nur Zugriff auf die IP-Bereiche und Protokolle, die Clients tatsächlich benötigen. Vermeiden Sie zu weit gefasste Regeln für Zugriffsquellen, die Ihre Infrastruktur unberechtigtem Zugriff aussetzen könnten.
- Wechseln Sie die Tokens regelmäßig — Ersetzen Sie Zugriffstoken regelmäßig, noch bevor sie ablaufen. Diese Vorgehensweise begrenzt die Auswirkungen kompromittierter Token und gewährleistet die Sicherheitshygiene.
- Zugriffsmuster überwachen — Überprüfen Sie die DNS-Abfrageprotokolle, um ungewöhnliche Zugriffsmuster oder potenzielle Sicherheitsprobleme zu identifizieren. Richten Sie Warnmeldungen für Abfragen aus unerwarteten IP-Bereichen oder für die Verwendung abgelaufener Token ein.

Bewährte betriebliche Verfahren

Halten Sie sich an die folgenden betrieblichen Verfahren, um zuverlässige Zugriffskontrollen aufrechtzuerhalten:

- Dokumentieren Sie Ihre Zugriffskontrollstrategie — Sorgen Sie für eine klare Dokumentation darüber, welche Zugriffsquellen und Tokens welchen Kundengruppen dienen.
- Testen Sie die Zugriffskontrollen regelmäßig — Stellen Sie sicher, dass Ihre Regeln und Token für die Zugriffsquellen von verschiedenen Client-Standorten und in verschiedenen Szenarien aus korrekt funktionieren.
- Planen Sie die Token-Erneuerung — Richten Sie Prozesse für die Verteilung neuer Token ein, bevor alte ablaufen, um Serviceunterbrechungen zu vermeiden.
- Überprüfen Sie die Zugriffskontrollen regelmäßig — Entfernen Sie ungenutzte Regeln für Zugriffsquellen und abgelaufene Token, um eine saubere Konfiguration zu gewährleisten.

DNS für Clients mit Route 53 Global Resolver sichern

In den folgenden Abschnitten wird beschrieben, wie Sie Regeln zum Schutz von DNS-Abfragen Ihrer Kunden erstellen.

Topics

DNS-Firewallregeln konfigurieren und verwalten

Firewallregeln erstellen und anzeigen

Firewallregeln definieren, wie Route 53 Global Resolver DNS-Abfragen verarbeitet, die auf Domänenlisten, verwalteten Domänenlisten, Inhaltskategorien oder erweitertem Bedrohungsschutz basieren. Jede Regel legt eine Priorität, Zieldomänen und eine zu ergreifende Aktion fest.

Bewährte Methoden für die Regelpriorität:

- Verwenden Sie die Priorität 100-999 für Zulassungsregeln mit hoher Priorität (vertrauenswürdige Domänen)
- Verwenden Sie die Priorität 1000-4999 für Blockregeln (bekannte Bedrohungen)
- Verwenden Sie die Priorität 5000-9999 für Warnregeln (Überwachung und Analyse)
- Lassen Sie Lücken zwischen den Prioritäten, um das Einfügen future Regeln zu ermöglichen

Um eine DNS-Firewallregel zu erstellen

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrer DNS-Ansicht.
2. Wählen Sie die Registerkarte Firewall-Regeln.
3. Wählen Sie Firewallregel erstellen.
4. Gehen Sie im Abschnitt Regeldetails wie folgt vor:
   a. Geben Sie unter Regelname einen aussagekräftigen Namen für die Regel ein (bis zu 128 Zeichen).
   b. (Optional) Geben Sie unter Regelbeschreibung eine Beschreibung für die Regel ein (bis zu 255 Zeichen).
5. Wählen Sie im Abschnitt Regelkonfiguration den Konfigurationstyp Regel aus:
   - Vom Kunden verwaltete Domainlisten — Verwenden Sie eine Domainliste, die Sie erstellen und verwalten
   - AWS verwaltete Domainlisten — Verwenden Sie von Amazon bereitgestellte Domainlisten, die Sie verwenden können
   - Erweiterter DNS-Firewall-Schutz — Wählen Sie aus einer Reihe von verwalteten Schutzmaßnahmen und geben Sie einen Vertrauensschwellenwert an
6. Wählen Sie unter Regelaktion die Aktion aus, die ausgeführt werden soll, wenn die Regel zutrifft:
   - Zulassen — Die DNS-Abfrage wurde gelöst
   - Warnung — Lässt die DNS-Abfrage zu, erzeugt aber eine Warnung
   - Blockieren — Die DNS-Abfrage ist blockiert
7. Wählen Sie Firewallregel erstellen.

Gehen Sie wie folgt vor, um die ihnen zugewiesenen Regeln anzuzeigen. Sie können die Regel und die Regeleinstellungen auch aktualisieren.

Um eine Regel anzuzeigen und zu aktualisieren

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrer DNS-Ansicht.
2. Wählen Sie die Registerkarte DNS-Firewall-Regeln.
3. Wählen Sie die Regel aus, die Sie anzeigen oder bearbeiten möchten, und wählen Sie Bearbeiten.
4. Auf der Regelseite können Sie Einstellungen anzeigen und bearbeiten.

Informationen zu den Werten für Regeln finden Sie unter the section called “Regeleinstellungen in der DNS-Firewall”.

So löschen Sie eine Regel

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrer DNS-Ansicht.
2. Wählen Sie die Registerkarte DNS-Firewall-Regeln.
3. Wählen Sie die Regel aus, die Sie löschen möchten, wählen Sie Löschen und bestätigen Sie den Löschvorgang.

Regeleinstellungen in der DNS-Firewall

Wenn Sie eine DNS-Firewallregel in Ihrer DNS-Ansicht erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Name

Eine eindeutige Kennung für die Regel in der DNS-Ansicht.

(Optionale) Beschreibung

Eine kurze Beschreibung, die weitere Informationen über die Regel enthält.

Domainliste

Die Liste der Domains, auf die die Regel überprüft. Sie können Ihre eigene Domainliste erstellen und verwalten oder Sie können eine Domainliste abonnieren, die für Sie AWS verwaltet wird.

Eine Regel kann entweder eine Domainliste oder einen erweiterten DNS-Firewall-Schutz enthalten, aber nicht beides.

Abfragetyp (nur Domänenlisten)

Die Liste der DNS-Abfragetypen, nach denen die Regel sucht. Die folgenden Werte sind gültig:

- A: Gibt eine IPv4 Adresse zurück.

- AAAA: Gibt eine IPv6-Adresse zurück.
- CAA: Einschränkungen, mit denen SSL/TLS Zertifizierungen für CAs die Domain erstellt werden können.
- CNAME: Gibt einen anderen Domainnamen zurück.
- DS: Datensatz, der den DNSSEC-Signaturschlüssel einer delegierten Zone identifiziert.
- MX: Spezifiziert Mailserver.
- NAPTR: Regular-expression-based Umschreiben von Domainnamen.
- NS: Autorisierende Nameserver.
- PTR: Ordnet eine IP-Adresse einem Domainnamen zu.
- SOA: Beginn des Autoritätsdatensatzes für die Zone.
- SPF: Listet die Server auf, die berechtigt sind, E-Mails von einer Domain aus zu versenden.
- SRV: Anwendungsspezifische Werte, die Server identifizieren.
- TXT: Überprüft E-Mail-Absender und anwendungsspezifische Werte.

Ein Abfragetyp, den Sie mithilfe der DNS-Typ-ID definieren, z. B. 28 für AAAA. Die Werte müssen als TYPE definiert seinNUMBER, wobei sie beispielsweise 1-65334 lauten NUMBER können. TYPE28 Weitere Informationen finden Sie unter Liste der DNS-Eintragstypen.

Sie können einen Abfragetyp pro Regel erstellen.

DNS Firewall Erweiterter Schutz

Erkennt verdächtige DNS-Abfragen auf der Grundlage bekannter Bedrohungssignaturen in DNS-Abfragen. Sie können zwischen folgenden Schutzoptionen wählen:

- Algorithmen zur Domain-Generierung (DGAs)

  DGAs werden von Angreifern verwendet, um eine große Anzahl von Domains zu generieren, um Malware-Angriffe zu starten.

- DNS-Tunneling

  DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.

In einer erweiterten DNS-Firewall-Regel können Sie wählen, ob Sie eine Anfrage, die der Bedrohung entspricht, blockieren oder bei einer Warnung warnen möchten.

Weitere Informationen finden Sie unter Erweiterter Schutz durch die DNS-Firewall.

Eine Regel kann entweder einen erweiterten DNS-Firewall-Schutz oder eine Domänenliste enthalten, aber nicht beides.

Vertrauensschwellenwert (nur DNS Firewall Advanced)

Der Vertrauensschwellenwert für DNS Firewall Advanced. Sie müssen diesen Wert angeben, wenn Sie eine Regel für DNS Firewall Advanced erstellen. Die Werte für das Vertrauensniveau bedeuten:

- Hoch – Erkennt nur die am besten bestätigten Bedrohungen bei einer niedrigen Rate an falsch-positiven Alarmen.
- Mittel – Sorgt für ein ausgewogenes Verhältnis zwischen der Erkennung von Bedrohungen und falsch-positiven Alarmen.
- Niedrig – Bietet die höchste Erkennungsrate für Bedrohungen, erhöht jedoch auch die Zahl der falsch-positiven Fehlalarme.

Weitere Informationen finden Sie unter Regeleinstellungen in der DNS-Firewall.

Action

Wie Sie möchten, dass die DNS-Firewall eine DNS-Abfrage verarbeitet, deren Domainname mit den Spezifikationen in der Domainliste der Regel übereinstimmt. Weitere Informationen finden Sie unter the section called “Regelaktionen in der DNS-Firewall”.

Priorität

Eindeutige positive Ganzzahleinstellung für die Regel in der DNS-Ansicht, die die Verarbeitungsreihenfolge bestimmt. Die DNS-Firewall überprüft DNS-Abfragen anhand der Regeln in einer DNS-Ansicht, beginnend mit der niedrigsten numerischen Prioritätseinstellung und aufwärts. Sie können die Priorität einer Regel jederzeit ändern, z. B. um die Reihenfolge der Verarbeitung zu ändern oder Platz für andere Regeln zu schaffen.

Regelaktionen in der DNS-Firewall

Wenn die DNS-Firewall eine Übereinstimmung zwischen einer DNS-Abfrage und einer Domainspezifikation in einer Regel findet, wendet sie die in der Regel angegebene Aktion auf die Abfrage an.

Sie müssen in jeder von Ihnen erstellten Regel eine der folgenden Optionen angeben:

- Zulassen — Beenden Sie die Überprüfung der Abfrage und lassen Sie sie durchgehen. Nicht verfügbar für DNS Firewall Advanced.

- Warnung — Beenden Sie die Überprüfung der Abfrage, lassen Sie sie durchlaufen und protokollieren Sie eine Warnung für die Abfrage in den Route 53 Resolver-Protokollen.
- Blockieren — Unterbrechen Sie die Überprüfung der Abfrage, verhindern Sie, dass sie zum vorgesehenen Ziel weitergeleitet wird, und protokollieren Sie die Blockaktion für die Abfrage in den Route 53 Resolver-Protokollen.

  Antworten Sie mit der konfigurierten Blockantwort wie folgt:

  - NODATA — Antwortet und gibt an, dass die Abfrage erfolgreich war, aber keine Antwort darauf verfügbar ist.
  - NXDOMAIN — Antwortet und gibt an, dass der Domainname der Anfrage nicht existiert.
  - OVERRIDE — Geben Sie in der Antwort eine benutzerdefinierte Überschreibung an. Für diese Option sind die folgenden zusätzlichen Einstellungen erforderlich:
    - Datensatzwert — Der benutzerdefinierte DNS-Eintrag, der als Antwort auf die Anfrage zurückgesendet werden soll.
    - Eintragstyp — Der Typ des DNS-Eintrags. Dies bestimmt das Format des Datensatzwertes. Dies muss `CNAME` lauten.
    - Gültigkeitsdauer in Sekunden — Die empfohlene Zeitspanne für den DNS-Resolver oder Webbrowser, um den Override-Eintrag zwischenzuspeichern und ihn als Antwort auf diese Anfrage zu verwenden, falls er erneut empfangen wird. Standardmäßig ist dies Null, und der Datensatz wird nicht zwischengespeichert.

Verwaltete Domänenlisten für Route 53 Global Resolver

Verwaltete Domänenlisten enthalten Domainnamen, die mit böswilligen Aktivitäten oder anderen potenziellen Bedrohungen in Verbindung stehen. AWS verwaltet diese Listen, damit Route 53 Global Resolver-Kunden bei der Verwendung der DNS-Firewall internetgebundene DNS-Abfragen mit ihnen vergleichen können.

Sich über die sich ständig ändernde Bedrohungslandschaft auf dem Laufenden zu halten, kann zeitaufwändig und teuer sein. Mit verwalteten Domänenlisten können Sie Zeit sparen, wenn Sie die DNS-Firewall auf Global Resolver implementieren und verwenden. AWS aktualisiert die Listen automatisch, wenn neue Sicherheitslücken und Bedrohungen auftauchen.

Verwaltete Domänenlisten sind in die Kategorien Bedrohung und Inhalt unterteilt. Diese dienen dazu, Sie vor gängigen Internet-Bedrohungen zu schützen und auch die Auflösung von Abfragen zu verhindern, die keine Domain betreffen safe-for-work.

Als bewährte Methode sollten Sie eine verwaltete Domainliste in einer Nicht-Produktionsumgebung testen, bevor Sie sie in der Produktion verwenden, wobei die Regelaktion auf `Alert` festgelegt ist. Evaluieren Sie die Regel anhand von CloudWatch Amazon-Metriken in Kombination mit gesampelten DNS-Firewall-Anfragen oder Global Resolver-Protokollen. Wenn Sie überzeugt sind, dass die Regel das tut, was Sie wollen, ändern Sie die Aktionseinstellung nach Bedarf.

Verfügbare AWS verwaltete Domainlisten

In diesem Abschnitt werden die verwalteten Domänenlisten beschrieben, die derzeit für Global Resolver verfügbar sind. AWS enthält die folgenden verwalteten Domänenlisten für alle Benutzer von Global Resolver, sortiert nach Bedrohung oder Inhaltstyp.

Bedrohungskategorien

Schadsoftware
Botnet/Befehl und Kontrolle
Aggregierte Bedrohungsliste
GuardDuty Amazon-Bedrohungsliste
Phishing
Spam

Inhaltskategorien

Gewalt und Hassreden
Für Kinder
Online-Werbung
Wissenschaft
Familie und Erziehung
Haustiere
Karriere und Jobsuche

Religion
Lebensstil
Haus und Garten
Kriminelle und illegale Aktivitäten
Sport und Freizeit
Fahrzeuge
Finanzdienstleistungen
Immobilien
Hobbys und Interessen
Reisen
Essen und Essen
Regierung und Recht
Bildung
Mode
Gesundheit
Einkaufen
Inhalte für Erwachsene und Erwachsene
Technologie und Internet
Geschäft und Wirtschaft
Neuigkeiten
Suchmaschinen und Portale

Kunst und Kultur
Unterhaltung
Militärisch
Soziale Netzwerke
Vermeidung von Proxys
Umleiten
Email
Übersetzung
Kindesmissbrauch
Abtreibung
Glücksspiel
Hacken
Marihuana
Kryptowährung
Datierung
Künstliche Intelligenz und Machine Learning
Geparkte Domains
Private IP-Adresse

Verwaltete Domänenlisten können nicht heruntergeladen oder durchsucht werden. Um geistiges Eigentum zu schützen, können Sie die einzelnen Domainspezifikationen in den verwalteten Domainlisten nicht einsehen oder bearbeiten. Diese Einschränkung trägt auch dazu bei, böswillige Benutzer daran zu hindern, Bedrohungen zu entwickeln, die speziell zur Umgehung veröffentlichter Listen dienen.

Erstellen Sie Listen mit Domains, die blockiert oder zugelassen werden sollen

Sie können eigene Domainlisten erstellen, um Domainkategorien anzugeben, die Sie entweder nicht in den verwalteten Domainlistenangeboten finden oder die Sie lieber selbst bearbeiten.

Zusätzlich zu den in diesem Abschnitt beschriebenen Verfahren können Sie in der Konsole eine Domänenliste im Kontext der Regelverwaltung der DNS-Firewall erstellen, wenn Sie eine Regel erstellen oder aktualisieren.

Jede Domainspezifikation in Ihrer Domainliste muss die folgenden Anforderungen erfüllen:

- Es kann optional mit * (Sternchen) beginnen.
- Mit Ausnahme des optionalen Anfangssterns und einem Punkt als Trennzeichen zwischen Kennzeichnungen, darf es nur die folgenden Zeichen enthalten: `A-Z`, `a-z`, `0-9`, `-` (Bindestrich).
- Es muss 1 bis 255 Zeichen lang sein.

Um eine Domänenliste zu erstellen

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrem Global Resolver.
2. Wählen Sie die Registerkarte Domainlisten.
3. Wählen Sie Domainliste erstellen.
4. Geben Sie einen Namen und eine optionale Beschreibung für Ihre Domainliste sowie alle Tags ein und wählen Sie Domainliste erstellen aus.
5. Sobald die Erstellung abgeschlossen und betriebsbereit ist, können Sie mit dem Hinzufügen von Domains zu Ihrer Domainliste beginnen, indem Sie Domains hinzufügen auswählen.
6. Wenn Sie eine Domainliste aus einem Amazon S3 S3-Bucket hochladen möchten, geben Sie die URI des Amazon S3 S3-Buckets ein, in dem Sie eine Domainliste erstellt haben. Diese Domainliste sollte einen Domainnamen pro Zeile haben.
7. Andernfalls geben Sie Ihre Domain-Spezifikationen in das Textfeld ein, eine pro Zeile.
8. Wählen Sie Domains hinzufügen.

Um eine Domainliste zu löschen

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrem Global Resolver.

2. Wählen Sie die Registerkarte Domainlisten.
3. Wählen Sie die zu löschende Domainliste aus, wählen Sie dann Löschen und bestätigen Sie den Löschvorgang.

DNS Firewall — Erweiterter Schutz

DNS Firewall Advanced erkennt verdächtige DNS-Abfragen auf der Grundlage bekannter Bedrohungssignaturen in DNS-Abfragen. Sie können einen Bedrohungstyp in einer Regel angeben, die Sie in einer DNS-Firewallregel verwenden, die einer DNS-Ansicht zugeordnet ist.

DNS Firewall Advanced identifiziert verdächtige DNS-Bedrohungssignaturen, indem es eine Reihe von Schlüsselkennungen in der DNS-Payload untersucht, darunter den Zeitstempel der Anfragen, die Häufigkeit von Anfragen und Antworten, die DNS-Abfragezeichenfolgen sowie die Länge, Art oder Größe sowohl ausgehender als auch eingehender DNS-Abfragen. Je nach Art der Bedrohungssignatur können Sie Richtlinien so konfigurieren, dass die Anfrage blockiert oder einfach protokolliert und eine Warnung angezeigt wird. Durch die Verwendung eines erweiterten Satzes von Bedrohungskennungen können Sie sich vor DNS-Bedrohungen schützen, die von Domänenquellen ausgehen, die möglicherweise noch nicht durch Threat-Intelligence-Feeds, die von der breiteren Sicherheitsgemeinschaft verwaltet werden, noch nicht klassifiziert wurden.

Derzeit bietet DNS Firewall Advanced Schutz vor:

- Algorithmen zur Domain-Generierung () DGAs

  DGAs werden von Angreifern verwendet, um eine große Anzahl von Domains zu generieren, um Malware-Angriffe zu starten.
- DNS-Tunneling

  DNS-Tunneling wird von Angreifern verwendet, um mithilfe des DNS-Tunnels Daten vom Client zu exfiltrieren, ohne eine Netzwerkverbindung zum Client herzustellen.

Informationen zum Erstellen von Regeln finden Sie unter. the section called “DNS-Firewallregeln konfigurieren und verwalten”

Beseitigung von False-Positive-Szenarien

Wenn Sie in Regeln, die erweiterte DNS-Firewall-Schutzfunktionen zum Blockieren von Abfragen verwenden, auf falsch positive Szenarien stoßen, gehen Sie wie folgt vor:

1. Identifizieren Sie in den Global Resolver-Protokollen die Regel und die erweiterten Schutzmaßnahmen der DNS-Firewall, die die Fehlalarme verursacht haben. Dazu finden Sie das Protokoll für die Abfrage, die die DNS-Firewall blockiert, aber die Sie zulassen möchten. Im Protokolleintrag sind die DNS-Ansicht, die Regel, die Regelaktion und der erweiterte DNS-Firewall-Schutz aufgeführt.
2. Erstellen Sie in der DNS-Ansicht eine neue Regel, die die blockierte Abfrage explizit durchlässt. Wenn Sie die Regel erstellen, können Sie Ihre eigene Domainliste nur mit der Domainspezifikation definieren, die Sie zulassen möchten. Folgen Sie den Anleitungen zur Regelverwaltung unterthe section called “DNS-Firewallregeln konfigurieren und verwalten”.
3. Ordnen Sie der neuen Regel innerhalb der Regel Priorität zu, sodass sie vor der Regel ausgeführt wird, die die verwaltete Liste verwendet. Geben Sie dazu der neuen Regel eine niedrigere numerische Prioritätseinstellung.

Wenn Sie Ihre Regeln aktualisiert haben, erlaubt die neue Regel ausdrücklich den Domainnamen, den Sie zulassen möchten, bevor die Sperrregel ausgeführt wird.

DNS-Sicherheitsrichtlinien in Route 53 Global Resolver verwalten

Verwaltung globaler Resolver

Nachdem Sie einen globalen Resolver erstellt haben, können Sie dessen Details anzeigen, seine Konfiguration bearbeiten und die zugehörigen Ressourcen auf der Seite Globale Resolver verwalten.

Details zum Resolver anzeigen

Auf der Seite Global Resolvers wird eine Liste all Ihrer Resolver mit wichtigen Informationen wie dem Namen des Resolvers, den bereitgestellten Regionen, den zugehörigen DNS-Ansichten, der Observability-Region und dem Betriebsstatus angezeigt.

Globale Resolver bearbeiten

Sie können den Namen und die Beschreibung des Resolvers nach der Erstellung ändern. Sie können die Regionen, in denen ein globaler Resolver bereitgestellt wird, nach der Erstellung nicht ändern.

Firewall-Regeln verwalten

Nachdem Sie Firewallregeln erstellt haben, können Sie deren Priorität ändern, ihre Konfiguration aktualisieren oder sie nach Bedarf löschen.

Regelpriorität und Bewertungsreihenfolge

Firewallregeln werden in der Reihenfolge ihrer Priorität bewertet, wobei niedrigere Zahlen zuerst verarbeitet werden. Wenn eine Abfrage mehreren Regeln entspricht, wird nur die Aktion der ersten passenden Regel angewendet.

Firewall-Regeln werden aktualisiert

Sie können die meisten Aspekte einer Firewallregel nach der Erstellung aktualisieren, einschließlich ihrer Priorität, Aktion und Zieldomänen.

Konfiguration von Zuordnungen für private gehostete Zonen mit Route 53 Global Resolver

Mit Route 53 Global Resolver können Sie Datensätze, die mit Ihren privaten gehosteten Zonen von Route 53 verknüpft sind, von Ihren autorisierten Clients auflösen. Sie können die privat gehosteten Zonen von Route 53 der DNS-Ansicht zuordnen, die Ihre mit der DNS-Ansicht autorisierten Clients auflösen dürfen.

Topics

Verwalten Sie private gehostete Zonenzuordnungen mit Route 53 Global Resolver

Private Hosting-Zonen für interne Anwendungen erstellen

Bevor Sie eine private gehostete Zone mit einer DNS-Ansicht verknüpfen können, müssen Sie die Zone zunächst mithilfe der Amazon Route 53-Konsole oder API erstellen.

Um eine private gehostete Zone zu erstellen

1. Öffnen Sie die Amazon Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie Erstellte gehostete Zone.
4. Geben Sie unter Domainname den Domainnamen für Ihre private Zone ein (z. B.`internal.example.com`).

5. Wählen Sie in der Liste Typ die Option Privat gehostete Zone.
6. Wählen VPCs Sie für die Verknüpfung mit der Hosting-Zone die aus, die VPCs Sie der Hosting-Zone zuordnen möchten. Optional können Sie die `CreateHostedZone` API-Operation verwenden, um die Eingabe eines Werts zu überspringen, da Sie die Zone stattdessen mit Route 53 Global Resolver verknüpfen.
7. Wählen Sie Erstellte gehostete Zone.

Nachdem Sie die private gehostete Zone erstellt haben, fügen Sie die DNS-Einträge hinzu, die Sie für Ihre internen Dienste benötigen.

Zuordnen von privat gehosteten Zonen zu DNS-Ansichten

Damit Route 53 Global Resolver Abfragen für Ihre private gehostete Zone auflösen kann, müssen Sie die Zone mit einer oder mehreren DNS-Ansichten verknüpfen.

Um eine private gehostete Zone einer DNS-Ansicht zuzuordnen

1. Navigieren Sie in der Route 53 Global Resolver-Konsole zu Ihrem globalen Resolver.
2. Wählen Sie die DNS-Ansicht aus, der Sie die private gehostete Zone zuordnen möchten.
3. Wählen Sie im Abschnitt Private gehostete Zonen die Option Gehostete Zone zuordnen aus.
4. Wählen Sie unter Gehostete Zone die private Hosting-Zone aus, die Sie zuordnen möchten.
5. Geben Sie unter Assoziationsname einen aussagekräftigen Namen für diese Zuordnung ein.
6. Wählen Sie „Gehostete Zone zuordnen“ aus.

Der Zuordnungsvorgang dauert in der Regel einige Minuten. Sobald der Vorgang abgeschlossen ist, verwendet Route 53 Global Resolver die Datensätze in der privaten Hosting-Zone, um DNS-Anfragen von Client-Geräten zu beantworten, die mit der DNS-Ansicht verknüpft sind.

Überwachung der DNS-Aktivität und -Leistung mit Route 53 Global Resolver

Route 53 Global Resolver bietet umfassende Einblicke in die DNS-Aktivitäten in Ihrem Unternehmen und ermöglicht es Ihnen, Sicherheitsbedrohungen zu identifizieren, das Verhalten von Client-Geräten zu analysieren und die Einhaltung von Vorschriften sicherzustellen. In diesem Kapitel werden sowohl die verfügbaren Überwachungstools als auch detaillierte Verfahren für die Einrichtung der DNS-

Überwachung, die Konfiguration von Protokollierungszielen und die Analyse von DNS-Daten zur Untersuchung von Bedrohungen und zur Leistungsoptimierung beschrieben.

AWS stellt diese Überwachungstools zur Verfügung, mit denen Sie einen sicheren und zuverlässigen DNS-Dienst aufrechterhalten können:

- Amazon CloudWatch verfolgt DNS-Abfragevolumen, Antwortzeiten und Sicherheitsereignisse in Echtzeit. Erstellen Sie Dashboards, um die DNS-Leistung standortübergreifend zu überwachen, und richten Sie Alarme ein, um Sie zu benachrichtigen, wenn das Abfragevolumen steigt oder sich die von Ihnen angegebenen Antwortzeiten verlängern. Für Route 53 Global Resolver können Sie das Abfragevolumen, die Antwortzeiten und die Filteraktivität überwachen. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von EC2 Amazon-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. Route 53 Global Resolver kann CloudWatch DNS-Abfrageprotokolle zur Überwachung und Analyse in Echtzeit direkt an Logs übermitteln. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Topics

Verschaffen Sie sich mit Route 53 Global Resolver einen Überblick über die DNS-Aktivitäten

Route 53 Global Resolver bietet umfassende Funktionen zur Protokollierung von DNS-Abfragen, um die Aktivität von Client-Geräten zu überwachen und Sicherheitsbedrohungen zu identifizieren. Aktivieren Sie die DNS-Abfrageprotokollierung in Route 53 Global Resolver, um zu sehen, auf welche Websites Client-Geräte zugreifen, um potenzielle Sicherheitsbedrohungen zu identifizieren und DNS-Auflösungsmuster zu analysieren. In den Protokollen werden umfassende Informationen zu jeder Abfrage erfasst, einschließlich der angewendeten Sicherheitsrichtlinien.

Welche Informationen werden in DNS-Protokollen erfasst

Jeder DNS-Abfrageprotokolleintrag enthält detaillierte Informationen zur Aktivität auf Client-Geräten und zur Durchsetzung von Sicherheitsrichtlinien:

- Abfrageinformationen — Domänenname, Abfragetyp, Abfrageklasse und verwendetes Protokoll
- Informationen zum Client-Gerät — Quell-IP-Adresse, DNS-Ansicht und Authentifizierungsmethode
- Antwortinformationen — Antwortcode, Antwortdatensätze und Antwortzeit
- Sicherheitsaktionen — Übereinstimmungen mit Firewallregeln, Ergebnisse der Bedrohungserkennung und ergriffene Maßnahmen
- Metadaten — Zeitstempel, globale Resolver-ID, Region und Ablaufverfolgungsinformationen

OCSF-Format für die Sicherheitsintegration

DNS-Abfrageprotokolle verwenden das Open Cybersecurity Schema Framework (OCSF), das ein standardisiertes Format für Daten zu Sicherheitsereignissen bietet. Dieses Format ermöglicht:

- Standardisierte Analyse — Konsistentes Schema für verschiedene Sicherheitstools
- Verbesserte Interoperabilität — Einfache Integration mit SIEM- und Analyseplattformen
- Verbesserte Korrelation — Fähigkeit, DNS-Ereignisse mit anderen Sicherheitsdaten zu korrelieren
- Zukünftige Kompatibilität — Support für sich ändernde Sicherheitsanalyseanforderungen

Beispiele für das OCSF-Protokollformat

Route 53 Global Resolver DNS-Abfrageprotokolle folgen der OCSF-Schemastruktur und bieten detaillierte Informationen zu jeder DNS-Abfrage, Antwort und Sicherheitsaktion. Die folgenden Beispiele zeigen das Protokollformat für zulässige und abgelehnte Abfragen.

Route 53 Global Resolver DNS-Protokoll — Beispiel für erlaubten Zugriff

Dieses Beispiel zeigt eine DNS-Abfrage, die durch Firewallregeln zugelassen wurde. Das Protokoll enthält Abfragedetails, Antwortinformationen und Anreicherungsdaten mit Route 53 Global Resolver-spezifischen Identifikatoren.


```
{
    "action_id": 1,
    "action_name": "Allowed",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-east-1",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
        "direction": "Inbound",
        "direction_id": 1,
        "protocol_name": "udp",
        "protocol_num": 17,
        "protocol_ver": "",
        "uid": "db21d1739ddb423a"
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [{
        "rdata": "3.3.3.3",
        "type": "A",
        "class": "IN",
        "ttl": 300
```

```
    },
    {
        "rdata": "3.3.3.4",
        "type": "A",
        "class": "IN",
        "ttl": 300
    }],
    "src_endpoint": {
        "ip": "3.3.3.1",
        "port": 56576
    },
    "enrichments": [{
        "name": "global-resolver",
        "value": "gr-a1b2c3d4fexample",
        "data": {
            "dns_view_id": "dnsv-a1b2c3d4fexample",
            "firewall_rule_id": "fr-a1b2c3d4fexample",
            "token_id": "t-a1b2c3d4fexample",
            "token_name": "device-123456",
            "token_expiration": "1789419206",
        }
    }],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
            }
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "NOERROR",
    "rcode_id": 0,
    "response_time": 1761358379995,
```

```
    "severity": "Informational",
    "severity_id": 1,
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "start_time": 1761358379995,
    "status": "Success",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```


Route 53 Global Resolver DNS-Protokoll — Beispiel für Zugriff verweigert

Dieses Beispiel zeigt eine DNS-Abfrage, die durch Firewallregeln blockiert wurde. Das Protokoll enthält die Ablehnungsaktion, ein leeres Antwortfeld und den REFUSED-Antwortcode, der angibt, dass die Abfrage nicht verarbeitet wurde.


```
{
    "action_id": 2,
    "action_name": "Denied",
    "activity_id": 6,
    "activity_name": "Traffic",
    "category_name": "Network Activity",
    "category_uid": 4,
    "class_name": "DNS Activity",
    "class_uid": 4003,
    "cloud": {
        "provider": "AWS",
        "region": "us-west-2",
        "account": {
            "uid": "123456789012"
        }
    },
    "connection_info": {
        "direction": "Inbound",
        "direction_id": 1,
        "protocol_name": "tcp",
        "protocol_num": 6,
        "protocol_ver_id": 4,
        "uid": "9fdc6fbc09794d5e"
```

```
    },
    "duration": 1,
    "end_time": 1761358379996,
    "answers": [],
    "src_endpoint": {
        "ip": "3.3.3.3",
        "port": 28276
    },
    "enrichments": [
        {
            "name": "global-resolver",
            "value": "gr-a1b2c3d4fexample",
            "data": {
                "dns_view_id": "dnsv-a1b2c3d4fexample",
                "firewall_rule_id": "fr-a1b2c3d4fexample",
                "token_id": "t-a1b2c3d4fexample",
                "token_name": "device-123456",
                "token_expiration": "1789419206",
            }
        }
    ],
    "message": "",
    "metadata": {
        "version": "1.2.0",
        "product": {
            "name": "Global Resolver",
            "vendor_name": "AWS",
            "feature": {
                "name": "DNS"
            }
        }
    },
    "query": {
        "hostname": "example.com.",
        "class": "IN",
        "type": "A",
        "opcode": "Query",
        "opcode_id": 0
    },
    "query_time": 1761358379995,
    "rcode": "REFUSED",
    "rcode_id": 5,
    "response_time": 1761358379995,
    "severity": "Informational",
```

```
    "severity_id": 1,
    "start_time": 1761358379995,
    "status": "Failure",
    "status_id": 1,
    "time": 1761358379995,
    "type_name": "DNS Activity: Traffic",
    "type_uid": 400306
}
```


Konfigurieren Sie die DNS-Überwachung und -Protokollierung mit Route 53 Global Resolver

Konfigurieren Sie die DNS-Überwachung in Route 53 Global Resolver, um detaillierte Informationen zu DNS-Abfragen, Antworten und Sicherheitsaktionen zu erfassen. In diesem Abschnitt werden die Schritte zum Einrichten von Protokollierungszielen und zum Konfigurieren von Überwachungstools beschrieben.

Einstellung der Observability-Region

Bevor Sie die DNS-Protokollierung konfigurieren, müssen Sie eine Observability-Region festlegen, in der Protokolle und Metriken gespeichert werden. Diese Region bestimmt, wo Ihre Überwachungsdaten verarbeitet und gespeichert werden.

1. Öffnen Sie die Route 53 Global Resolver-Konsole unter https://console.aws.amazon.com/route53globalresolver/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im Abschnitt Observability-Region die Option Region festlegen aus.
4. Wählen Sie die AWS Region aus, in der Sie die Monitoring-Daten speichern möchten, und wählen Sie dann Region festlegen aus.

Nachdem Sie die Observability-Region festgelegt haben, können Sie die Ziele für die Protokollzustellung in dieser Region konfigurieren.

Behebung von DNS-Problemen mit Route 53 Global Resolver

Route 53 Global Resolver bietet umfassende DNS-Auflösungsfunktionen, aber gelegentlich müssen Sie möglicherweise Verbindungs-, Leistungs- oder Konfigurationsprobleme beheben. Verwenden Sie DNS-Protokolle, Überwachungsdaten und Diagnosetechniken, um Probleme zu identifizieren

und zu lösen, die sich auf die DNS-Auflösung von Client-Geräten mit Route 53 Global Resolver auswirken. Dieses Kapitel bietet systematische Ansätze zur Behebung häufiger DNS-Probleme und zur Leistungsoptimierung.

Topics

Diagnostizieren Sie DNS-Konnektivitätsprobleme mit Route 53 Global Resolver

Route 53 Global Resolver bietet eine zuverlässige DNS-Auflösung, aber gelegentlich können Verbindungsprobleme aufgrund von Konfigurations-, Authentifizierungs- oder Netzwerkproblemen auftreten. Wenn Client-Geräte Domänennamen mit Route 53 Global Resolver nicht auflösen können, verwenden Sie diese systematischen Ansätze, um Verbindungsprobleme zu identifizieren und zu lösen.

Client-Geräte können Domänen nicht auflösen

Gehen Sie wie folgt vor, um Auflösungsfehler zu diagnostizieren:

1. Stellen Sie sicher, dass Anfragen den globalen Resolver erreichen
   - Suchen Sie in den DNS-Abfrageprotokollen nach Abfragen von der IP-Adresse des betroffenen Client-Geräts
   - Vergewissern Sie sich, dass das Client-Gerät mit den richtigen Anycast-IP-Adressen konfiguriert ist
   - Testen Sie die Netzwerkkonnektivität vom Client-Gerät zum Anycast IPs
2. Überprüfen Sie die Authentifizierung des Client-Geräts
   - Stellen Sie sicher, dass das Client-Gerät mit der richtigen DNS-Ansicht authentifiziert ist
   - Überprüfen Sie die Zugriffsquellenregeln für die IP-Adresse oder den CIDR-Block des Client-Geräts
   - Vergewissern Sie sich, dass die Zugriffstoken gültig und nicht abgelaufen sind (für tokenbasierte Authentifizierung)

3. Überprüfen Sie die Firewall-Regeln
   - Prüfen Sie, ob die Firewallregeln die Abfragen blockieren
   - Überprüfen Sie die Regelpriorität und stellen Sie sicher, dass Zulassungsregeln eine höhere Priorität haben als Blockregeln
   - Überprüfen Sie die Einstellungen für das Fail-Open-Verhalten der Firewall
4. Bestätigen Sie die DNS-View-Verknüpfungen
   - Überprüfen Sie die Zuordnungen privater gehosteter Zonen für interne Domänen
   - Überprüfen Sie, ob DNS-Einträge in den zugehörigen privaten Hosting-Zonen vorhanden sind
   - Stellen Sie sicher, dass die Domainnamen in Abfragen genau mit den Zonennamen übereinstimmen

Zeitweise auftretende Auflösungsfehler

Untersuchen Sie bei sporadischen DNS-Auflösungsproblemen die folgenden möglichen Ursachen:

Probleme bei der Authentifizierung

- Suchen Sie nach Ablauf- und Verlängerungsmustern für Zugriffstoken
- Überprüfen Sie die Authentifizierungsprotokolle auf fehlgeschlagene Authentifizierungsversuche
- Überprüfen Sie die Uhrsynchronisierung des Client-Geräts für die Tokenvalidierung

Netzwerkkonnektivität

- Achten Sie auf Netzwerkpfadänderungen oder Routing-Probleme
- Suchen Sie nach Änderungen der Firewall- oder NAT-Gerätekonfiguration
- Stellen Sie sicher, dass das Anycast-Routing zur nächstgelegenen Region konsistent ist

Servicezustand

- Überprüfen Sie das AWS Service Health Dashboard auf Probleme mit Route 53 Global Resolver
- Überprüfen Sie die CloudWatch Metriken auf Spitzenwerte bei der Fehlerrate
- Überwachen Sie den Zuordnungsstatus der privaten gehosteten Zone

Unerwartete öffentliche Lösung

Wenn Abfragen in öffentliches DNS statt in privat gehostete Zonen aufgelöst werden:

1. Überprüfen Sie die Konfiguration der privaten gehosteten Zone
   - Vergewissern Sie sich, dass die private gehostete Zone die erwarteten DNS-Einträge enthält
   - Vergewissern Sie sich, dass die Namen der Datensätze exakt mit der abgefragten Domain übereinstimmen
   - Stellen Sie sicher, dass die Datensatztypen mit dem Abfragetyp übereinstimmen (A, AAAA, CNAME usw.)
2. Überprüfen Sie die Zuordnungen der DNS-Ansicht
   - Stellen Sie sicher, dass die private gehostete Zone mit der richtigen DNS-Ansicht verknüpft ist
   - Vergewissern Sie sich, dass das Client-Gerät für die DNS-Ansicht authentifiziert ist
   - Überprüfen Sie den Zuordnungsstatus in der Konsole
3. Überprüfen Sie die Firewall-Regeln
   - Suchen Sie nach Firewallregeln, die möglicherweise Abfragen für private Zonen blockieren
   - Überprüfen Sie die Reihenfolge und Priorität der Regelauswertung
   - Überprüfen Sie die DNS-Abfrageprotokolle auf Firewall-Aktionen

Beheben Sie DNS-Leistungsprobleme mit Route 53 Global Resolver

Route 53 Global Resolver wurde für optimale Leistung mit globaler Anycast-Architektur entwickelt, aber verschiedene Faktoren können die DNS-Auflösungsgeschwindigkeit beeinflussen. Beheben Sie die langsame DNS-Auflösung und optimieren Sie die Antwortzeiten für Abfragen, um die Leistung der Client-Geräte mit Route 53 Global Resolver zu verbessern.

Langsame DNS-Auflösung

So diagnostizieren und beheben Sie langsame DNS-Antwortzeiten:

1. Analysieren Sie die Antwortzeiten von Abfragen
   - Verwenden Sie DNS-Abfrageprotokolle, um Abfragen mit hohen Antwortzeiten zu identifizieren
   - Vergleichen Sie die Antwortzeiten verschiedener Domänen und Abfragetypen
   - Überwachen Sie die Trends der Antwortzeiten im Zeitverlauf
2. Suchen Sie nach hohen Abfragevolumina
   - Überwachen Sie CloudWatch Metriken auf Spitzenwerte beim Abfragevolumen
   - Identifizieren Sie Client-Geräte oder DNS-Ansichten, die zu viele Abfragen generieren
   - Suchen Sie nach Abfragemustern, die auf Fehlkonfigurationen hinweisen könnten

3. Überprüfen Sie die Cache-Leistung
   - Analysieren Sie die Cache-Trefferquoten für häufig abgefragte Domains
   - Überprüfen Sie die TTL-Einstellungen für DNS-Einträge
   - Erwägen Sie, die TTL-Werte auf der Grundlage von Abfragemustern anzupassen
4. Überprüfen Sie die optimale Regionsauswahl
   - Stellen Sie sicher, dass sich die globalen Resolver-Regionen in der Nähe der Standorte der Client-Geräte befinden
   - Überwachen Sie das Anycast-Routing, um sicherzustellen, dass Anfragen die nächstgelegene Region erreichen
   - Erwägen Sie das Hinzufügen von Regionen, wenn die Client-Geräte geografisch weit entfernt sind

Strategien zur Leistungsoptimierung

Verwenden Sie diese Strategien, um die DNS-Leistung zu optimieren:

Cache-Optimierung

- Passen Sie die TTL-Werte auf der Grundlage von Abfragemustern und der Änderungshäufigkeit an
- Verwenden Sie länger TTLs für stabile Datensätze, kürzer TTLs für häufig wechselnde Datensätze
- Überwachen Sie die Cache-Trefferraten und passen Sie sie TTLs entsprechend an

Optimierung der Region

- Stellen Sie den globalen Resolver in Regionen bereit, die der Konzentration von Client-Geräten am nächsten kommen
- Überwachen Sie die Routingmuster und Antwortzeiten von Abfragen nach Regionen
- Erwägen Sie das Hinzufügen von Regionen für eine bessere geografische Abdeckung

Protokolloptimierung

- Wählen Sie die geeigneten DNS-Protokolle auf der Grundlage der Sicherheits- und Leistungsanforderungen
- Ziehen Sie DNS-over-HTTPS (DoH) für verschlüsselte Verbindungen mit Caching-Vorteilen in Betracht

- Verwenden Sie DNS-over-TLS (DoT) für verschlüsselte Verbindungen mit geringerem Overhead

Optimierung der Regeln

- Überprüfen und optimieren Sie die Priorität und Komplexität von Firewallregeln
- Ordnen Sie häufig übereinstimmende Regeln in der Prioritätsreihenfolge höher an
- Vereinfachen Sie komplexe Regelbedingungen, wo immer dies möglich ist

Beheben Sie Konfigurationsprobleme in Route 53 Global Resolver

Route 53 Global Resolver bietet umfangreiche Konfigurationsoptionen für DNS-Ansichten, Authentifizierung und Firewallregeln, was manchmal zu Konfigurationskonflikten oder Nichtübereinstimmungen führen kann. Identifizieren und lösen Sie häufig auftretende Konfigurationsprobleme mit Route 53 Global Resolver, die sich auf die DNS-Auflösung auswirken.

Probleme bei der Authentifizierung

Häufige Probleme und Lösungen bei der Authentifizierung:

Die Regeln für die Zugriffsquelle stimmen nicht überein

- Stellen Sie sicher, dass die IP-Adressen der Client-Geräte mit den konfigurierten CIDR-Blöcken übereinstimmen
- Suchen Sie nach NAT- oder Proxygeräten, die die Quell-IP-Adressen ändern
- Stellen Sie sicher, dass die Regeln für die Zugriffsquelle alle erwarteten IP-Bereiche der Client-Geräte abdecken

Fehler bei der Token-Authentifizierung

- Stellen Sie sicher, dass die Token auf den Client-Geräten korrekt konfiguriert sind
- Überprüfen Sie die Ablaufdaten und Verlängerungsprozesse von Tokens
- Stellen Sie sicher, dass die Uhren der Client-Geräte für die Token-Validierung synchronisiert sind

Die Protokolle stimmen nicht überein

- Stellen Sie sicher, dass die Client-Geräte Protokolle verwenden, die nach den Access Source-Regeln zulässig sind
- Stellen Sie sicher, dass die DoH- und DoT-Konfigurationen den Token-Protokollen entsprechen
- Stellen Sie sicher, dass die Firewallregeln die erforderlichen Protokolle nicht blockieren

Probleme mit der Konfiguration der DNS-Ansicht

Häufige Probleme mit der Konfiguration der DNS-Ansicht:

Falsche DNS-View-Verknüpfungen

- Stellen Sie sicher, dass die Client-Geräte für die vorgesehene DNS-Ansicht authentifiziert sind
- Vergewissern Sie sich, dass privat gehostete Zonen den richtigen DNS-Ansichten zugeordnet sind
- Überprüfen Sie die Firewallregeln, die auf jede DNS-Ansicht angewendet werden

Konflikte bei den DNS-Einstellungen

- Überprüfen Sie die DNSSEC-Validierungseinstellungen auf Kompatibilität mit Client-Geräten
- Überprüfen Sie die Einstellungen des EDNS-Client-Subnetzes auf Datenschutz und Leistungsgleichgewicht
- Stellen Sie sicher, dass das Verhalten der Firewall beim Fail-Open den Sicherheitsanforderungen entspricht

Probleme mit Firewall-Regeln

Häufige Probleme mit der Konfiguration von Firewallregeln:

Konflikte mit der Priorität von Regeln

- Überprüfen Sie die Reihenfolge der Regelauswertung und stellen Sie sicher, dass die Prioritäten korrekt zugewiesen sind
- Suchen Sie nach Blockregeln mit höherer Priorität als den vorgesehenen Zulassungsregeln
- Testen Sie Regeländerungen vor der Produktionsbereitstellung in einer kontrollierten Umgebung

Die Domänenliste stimmt nicht überein

- Überprüfen Sie die Domainspezifikationen in benutzerdefinierten Domainlisten
- Überprüfen Sie die Platzhaltermuster auf korrekte Syntax und Abdeckung
- Stellen Sie sicher, dass die Domainlisten aktualisiert und synchronisiert sind

Problembehandlung beim internen Ressourcenzugriff

Häufige Probleme und Lösungen bei der Verwaltung des Zugriffs auf interne Ressourcen:

Client-Geräte werden nicht in private Zoneneinträge aufgelöst

- Stellen Sie sicher, dass die private gehostete Zone der richtigen DNS-Ansicht zugeordnet ist
- Vergewissern Sie sich, dass das Client-Gerät für die richtige DNS-Ansicht authentifiziert ist
- Stellen Sie sicher, dass der Domänenname in der Abfrage genau mit dem Zonennamen übereinstimmt
- Stellen Sie sicher, dass die DNS-Einträge in der privaten Hosting-Zone vorhanden sind

Zeitweise auftretende Auflösungsfehler

- Überprüfen Sie den Zuordnungsstatus in der Konsole
- Überprüfen Sie die DNS-Abfrageprotokolle auf Fehlermuster
- Überprüfen Sie die Netzwerkkonnektivität zwischen Route 53 Global Resolver und Amazon Route 53

Unerwartete öffentliche Lösung

- Vergewissern Sie sich, dass die private gehostete Zone die erwarteten Datensätze enthält
- Suchen Sie nach Firewallregeln, die die Abfrage möglicherweise blockieren
- Stellen Sie sicher, dass die Anfrage von einem Client-Gerät stammt, das mit der DNS-Ansicht verknüpft ist

Kontingente für Route 53 Global Resolver

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. Sofern nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für Route 53 Global Resolver anzuzeigen, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS Dienste und dann Route 53 Global Resolver aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch zu Service Quotas. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Ihr AWS Konto hat die folgenden Kontingente für Route 53 Global Resolver.

Weiche Kontingente

In der folgenden Tabelle werden die Kontingente in Route 53 Global Resolver beschrieben, die erhöht werden können. Informationen zum Ändern von Kontingenten finden Sie unter Eine Kontingenterhöhung beantragen im Servicekontingents-Benutzerhandbuch.

Bei einigen Kunden kann es vorkommen, dass das Konto-Kontingent unter diesen veröffentlichten Kontingenten liegt. Wenn der Meinung sind, dass Sie den Fehler Resource limit exceeded (Ressourcenlimit überschritten) irrtümlich erhalten haben, verwenden Sie die Service Quotas-Konsole, um Kontingenterhöhungen zu beantragen.

Ressource	Standardkontingent	Einstellbar
Globale Resolver pro Konto	2	Ja
DNS-Aufrufe pro globalem Resolver	5	Ja
DNS-Aufrufe pro Konto	50	Ja
Domänenlisten pro Konto	1.000	Ja
Domains pro Domainliste	100 000	Ja
Domänen in einer Datei, die aus S3 importiert wurde	10.000	Ja
Anzahl der Domänen in allen Firewall-Regeln	1 000 000	Ja
Firewall-Regeln pro DNS-Ansicht	100	Ja
Zugriffstoken pro globalem Resolver	5,000	Ja
Zugriffsquellen pro globalem Resolver	1.000	Ja

Ressource	Standardkontingent	Einstellbar
CIDR-Größe der Zugriffsquellen pro globalem Resolver	65 000	Nein
Private gehostete Zonen pro DNS-Ansicht	1.000	Ja

Feste Kontingente

In der folgenden Tabelle werden Kontingente in Route 53 Global Resolver beschrieben, die nicht erhöht werden können.

Ressource oder Operation	Kontingent
Konfigurationen für die Protokollzustellung pro (globaler Resolver, Zieltyp, Region)	1

Erstellen von Amazon Route 53- und Route 53 VPC Resolver-Ressourcen mit AWS CloudFormation

Amazon Route 53 und Route 53 VPC Resolver sind in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.

Wenn Sie es verwenden CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Route 53- und VPC Resolver-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren Regionen bereit AWS-Konten .

Route 53, VPC Resolver und Vorlagen CloudFormation

Um Ressourcen für Route 53, VPC Resolver und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie Vorlagen verstehen CloudFormation . Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. CloudFormation Weitere Informationen finden Sie unter Was ist CloudFormation Designer? im AWS CloudFormation Benutzerhandbuch.

Route 53 unterstützt die Erstellung der folgenden Ressourcentypen in CloudFormation:

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für diese Route 53-Ressourcen, finden Sie in der Amazon-Route-53-Referenz zum RDS-Ressourcentyp im AWS CloudFormation -Benutzerhandbuch.

VPC Resolver unterstützt die Erstellung der folgenden Ressourcentypen in: 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`

Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für VPC-Resolver-Ressourcen, finden Sie in der Referenz zum Route 53 53-VPC-Resolver-Ressourcentyp im Benutzerhandbuch.AWS CloudFormation

Bewährte Methoden für Route 53 und CloudFormation

Beachten Sie CloudFormation bei der Verwaltung von Route 53-Ressourcen diese bewährten Methoden, um häufig auftretende Probleme zu vermeiden und zuverlässige Bereitstellungen sicherzustellen.

Verständnis der eventuellen Konsistenz

Route 53 verwendet ein eventuell konsistentes Modell für DNS-Änderungen. Dies kann sich auf den CloudFormation Betrieb auswirken, insbesondere bei Rollbacks und schnellen aufeinanderfolgenden Änderungen.

> **Important**
>
> Wenn CloudFormation versucht wird, DNS-Datensatzänderungen rückgängig zu machen, schlägt das Rollback möglicherweise aufgrund des Konsistenzmodells von Route 53 fehl. Wenn CloudFormation versucht wird, einen Datensatz neu zu erstellen, der vor Kurzem

gelöscht wurde, aber aufgrund einer eventuellen Konsistenz immer noch zu existieren scheint, können `InvalidChangeBatch` Fehler auftreten, die dazu führen, dass Ihr DNS defekt ist.

Gehen Sie wie folgt vor, um Probleme im Zusammenhang mit der eventuellen Konsistenz zu minimieren:

- Planen Sie Änderungen sorgfältig — Vermeiden Sie schnelle, aufeinanderfolgende Änderungen an denselben DNS-Einträgen
- Testen Sie zuerst außerhalb der Produktion — Testen Sie DNS-Änderungen immer in Entwicklungsumgebungen, bevor Sie sie in der Produktionsumgebung anwenden
- Bereitstellungen überwachen — Beobachten Sie CloudFormation Stack-Ereignisse bei DNS-bezogenen Bereitstellungen genau. Hinweise zur Überwachung finden Sie unter. Amazon Route 53 überwachen
- Halten Sie die Rollback-Verfahren bereit — Bereiten Sie manuelle Wiederherstellungsverfahren für den Fall vor, dass automatische Rollbacks fehlschlagen

Reihenfolge der DNS-Einträge und logische Reihenfolge IDs

Achten Sie beim Erstellen mehrerer DNS-Einträge auf CloudFormation die Reihenfolge der Datensätze und die logische ID-Zuweisung.

> **Warning**
>
> Wenn Sie DNS-Einträge in Arrays oder Listen innerhalb Ihrer CloudFormation Vorlage definieren, kann das Einfügen neuer Einträge in der Mitte der Liste dazu führen, dass bestehende Einträge logisch IDs neu CloudFormation zugewiesen werden. Dadurch werden Datensätze ersetzt, was zu Betriebsunterbrechungen und Rollback-Fehlern führen kann.

Bewährte Methoden für die Verwaltung von DNS-Einträgen:

- Explizit logisch verwenden IDs — Weisen Sie DNS-Einträgen immer explizite, aussagekräftige logische Daten IDs zu, anstatt sich auf Array-Indizes zu verlassen. Weitere Informationen zu CloudFormation Logical IDs finden Sie im AWS CloudFormation Benutzerhandbuch im Abschnitt „Ressourcen“

- Neue Einträge anhängen — Wenn Sie neue DNS-Einträge zu bestehenden Listen hinzufügen, fügen Sie sie am Ende an, anstatt sie in der Mitte einzufügen
- Zusammengehörende Datensätze gruppieren — Erwägen Sie die Verwendung `AWS::Route53::RecordSetGroup` für die gemeinsame Verwaltung verwandter Datensätze. Weitere Informationen finden Sie unter AWS::Route53::RecordSetGruppe im AWS CloudFormation Benutzerhandbuch.
- Änderungssätze überprüfen — Überprüfen Sie die CloudFormation Änderungssätze vor der Bereitstellung immer, um unerwartete Ersetzungen von Datensätzen zu identifizieren. Weitere Informationen finden Sie unter Aktualisieren von Stacks mithilfe von Änderungssets im AWS CloudFormation -Benutzerhandbuch.

Behandlung von Rollback-Fehlern

Wenn ein CloudFormation Rollback aufgrund von DNS-Problemen fehlschlägt, müssen Sie möglicherweise eine manuelle Wiederherstellung durchführen.

Um eine manuelle Wiederherstellung nach fehlgeschlagenen DNS-Rollbacks durchzuführen

1. Identifizieren Sie die fehlerhaften DNS-Einträge, indem Sie die CloudFormation Stack-Ereignisse und die Einträge für die gehostete Route 53-Zone überprüfen
2. Erstellen oder aktualisieren Sie die fehlenden DNS-Einträge manuell über die Route 53-Konsole oder API. Informationen zum Erstellen von Einträgen finden Sie unterArbeiten mit Datensätzen.
3. Sobald DNS wiederhergestellt ist, aktualisieren Sie Ihre CloudFormation Vorlage, sodass sie dem aktuellen Status entspricht
4. Stellen Sie die korrigierte Vorlage bereit, um sie CloudFormation wieder mit den tatsächlichen Ressourcen zu synchronisieren

Um Rollback-Fehler zu verhindern:

- Vermeiden Sie Änderungen, die dazu führen könnten, dass DNS-Einträge in Zeiten mit hohem Datenverkehr ersetzt werden
- Implementieren Sie Integritätsprüfungen und Überwachungen, um DNS-Probleme schnell zu erkennen. Informationen zu Integritätsprüfungen finden Sie unterErstellen und Aktualisieren von Zustandsprüfungen.

- Erwägen Sie die Verwendung von blaugrünen Bereitstellungsstrategien für kritische DNS-Änderungen. Weitere Informationen zu bewährten Bereitstellungsmethoden finden Sie unterBewährte Methoden für Amazon Route 53.
- Dokumentieren Sie Notfallverfahren für die manuelle DNS-Wiederherstellung

Erfahren Sie mehr über CloudFormation

Weitere Informationen CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- CloudFormation API Reference
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Codebeispiele für Route 53 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Route 53 mit einem AWS Software Development Kit (SDK) verwendet wird.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- ListPricesMit einem AWS SDK verwenden
- Verwendung RegisterDomain mit einem AWS SDK oder CLI
- Verwendung ViewBilling mit einem AWS SDK oder CLI

Codebeispiele für Route 53 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Route 53 mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien anzeigen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Grundlegende Beispiele für Route 53 mit AWS SDKs
  - Aktionen für Route 53 mit AWS SDKs
    - Verwendung von ChangeResourceRecordSets mit einer CLI
    - Verwendung von CreateHostedZone mit einer CLI
    - Verwendung von DeleteHostedZone mit einer CLI
    - Verwendung von GetHostedZone mit einer CLI
    - Verwendung ListHostedZones mit einem AWS SDK oder CLI
    - Verwendung von ListHostedZonesByName mit einer CLI
    - Verwendung von ListQueryLoggingConfigs mit einer CLI

Grundlegende Beispiele für Route 53 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie die Grundlagen von Amazon Route 53 mit verwenden können AWS SDKs.

Beispiele

- Aktionen für Route 53 mit AWS SDKs

- Verwendung von ChangeResourceRecordSets mit einer CLI
- Verwendung von CreateHostedZone mit einer CLI
- Verwendung von DeleteHostedZone mit einer CLI
- Verwendung von GetHostedZone mit einer CLI
- Verwendung ListHostedZones mit einem AWS SDK oder CLI
- Verwendung von ListHostedZonesByName mit einer CLI
- Verwendung von ListQueryLoggingConfigs mit einer CLI

Aktionen für Route 53 mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Route 53-Aktionen mit ausgeführt AWS SDKs werden. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der API-Referenz für Amazon Route 53.

Beispiele

- Verwendung von ChangeResourceRecordSets mit einer CLI
- Verwendung von CreateHostedZone mit einer CLI
- Verwendung von DeleteHostedZone mit einer CLI
- Verwendung von GetHostedZone mit einer CLI
- Verwendung ListHostedZones mit einem AWS SDK oder CLI
- Verwendung von ListHostedZonesByName mit einer CLI
- Verwendung von ListQueryLoggingConfigs mit einer CLI

Verwendung von **`ChangeResourceRecordSets`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `ChangeResourceRecordSets` verwendet wird.

CLI

AWS CLI

So erstellen, aktualisieren oder löschen Sie einen Ressourcendatensatz

Der folgende `change-resource-record-sets`-Befehl erstellt einen Ressourcendatensatz unter Verwendung der `hosted-zone-id` `Z1R8UBAEXAMPLE` und der JSON-formatierten Konfiguration in der Datei `C:\awscli\route53\change-resource-record-sets.json`:

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Weitere Informationen finden Sie unter POST ChangeResourceRecordSets in der Amazon Route 53 API-Referenz.

Die Konfiguration in der JSON-Datei hängt von der Art des Ressourceneintragssatzes ab, den Sie erstellen möchten:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Basissyntax

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Gewichtete Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
```

```
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Alias-Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
```

```
    },
    {...}
  ]
}
```

Gewichtete Alias-Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Latenz-Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
```

```
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Latenz-Alias-Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Failover-Syntax:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Syntax des Failover-Alias:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
```

```
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

- Einzelheiten zur API finden Sie ChangeResourceRecordSetsin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird ein A-Eintrag für www.example.com erstellt und der A-Eintrag für test.example.com von 192.0.2.3 in 192.0.2.1 geändert. Beachten Sie, dass Werte für Änderungen an TXT-Datensätzen in doppelten Anführungszeichen stehen müssen. Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Sie können das Get-R53Change Cmdlet verwenden, um abzufragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
```

```
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

Beispiel 2: Dieses Beispiel zeigt, wie Alias-Ressourceneinträge erstellt werden. „Z222222222“ ist die ID der von Amazon Route 53 gehosteten Zone, in der Sie den Alias-Ressourceneintragssatz erstellen. „example.com“ ist der Zonenapex, für den Sie einen Alias erstellen möchten, und „www.example.com“ ist eine Subdomain, für die Sie ebenfalls einen Alias erstellen möchten. 'Z1111111111111' ist ein Beispiel für eine Hosting-Zonen-ID für den Load Balancer und 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com' ist ein Beispiel für einen Load Balancer-Domainnamen, mit dem Amazon Route 53 auf Anfragen für example.com und www.example.com antwortet. Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Sie können das Cmdlet verwenden, um abzufragen, wann die Änderungen abgeschlossen sind. Get-R53Change

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
```

```
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Beispiel 3: In diesem Beispiel werden zwei A-Einträge für www.example.com erstellt. In einem Viertel der Fälle (1/(1+3)) antwortet Amazon Route 53 auf Anfragen für www.example.com mit den beiden Werten für den ersten Ressourceneintrag (192.0.2.9 und 192.0.2.10). In drei Viertel der Fälle (3/(1+3)) antwortet Amazon Route 53 auf Anfragen für www.example.com mit den beiden Werten für den zweiten Ressourceneintrag (192.0.2.11 und 192.0.2.12). Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Mit dem Get-R53Change Cmdlet können Sie abfragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
```

```
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Beispiel 4: Dieses Beispiel zeigt, wie gewichtete Alias-Ressourcendatensätze erstellt werden, vorausgesetzt, dass example.com die Domain ist, für die Sie gewichtete Alias-Ressourcendatensätze erstellen möchten. SetIdentifier unterscheidet die beiden gewichteten Alias-Ressourcendatensätze voneinander. Dieses Element ist erforderlich, da die Elemente „Name“ und „Type“ für beide Ressourceneintragsätze dieselben Werte haben. Z111111111111111 und Z3333333333333 sind Beispiele für gehostete Zonen für den ELB-Load Balancer, angegeben durch den Wert von. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com und example-load-balancer -4444444444.us-east-1.elb.amazonaws.com sind Beispiele für Elastic Load Balancing Balancing-Domains, von denen Amazon Route 53 auf Anfragen für example.com antwortet. Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Sie können das Cmdlet verwenden, um abzufragen, wann die Änderungen Get-R53Change abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
```

```
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Beispiel 5: In diesem Beispiel werden zwei Latenz-Alias-Ressourceneinträge erstellt, einer für einen ELB-Load Balancer in der Region US-West (Oregon) (us-west-2) und einer für einen Load Balancer in der Region Asien-Pazifik (Singapur) (ap-southeast-1). Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Mit dem Get-R53Change Cmdlet können Sie abfragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
```

```
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- Einzelheiten zur API finden Sie unter ChangeResourceRecordSets AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: In diesem Beispiel wird ein A-Eintrag für www.example.com erstellt und der A-Eintrag für test.example.com von 192.0.2.3 in 192.0.2.1 geändert. Beachten Sie, dass Werte für Änderungen an TXT-Datensätzen in doppelten Anführungszeichen stehen müssen. Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Sie können das Get-R53Change Cmdlet verwenden, um abzufragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
```

```
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords = @()
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

Beispiel 2: Dieses Beispiel zeigt, wie Alias-Ressourceneinträge erstellt werden. „Z222222222“ ist die ID der von Amazon Route 53 gehosteten Zone, in der Sie den Alias-Ressourceneintragssatz erstellen. „example.com“ ist der Zonenapex, für den Sie einen Alias erstellen möchten, und „www.example.com“ ist eine Subdomain, für die Sie ebenfalls einen Alias erstellen möchten. 'Z1111111111111' ist ein Beispiel für eine Hosting-Zonen-ID für den Load Balancer und 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com' ist ein Beispiel für einen Load Balancer-Domainnamen, mit dem Amazon Route 53 auf Anfragen für example.com und www.example.com antwortet. Weitere Informationen finden Sie in der

Dokumentation zu Amazon Route 53 Sie können das Cmdlet verwenden, um abzufragen, wann die Änderungen abgeschlossen sind. Get-R53Change

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Beispiel 3: In diesem Beispiel werden zwei A-Einträge für www.example.com erstellt. In einem Viertel der Fälle (1/(1+3)) antwortet Amazon Route 53 auf Anfragen für www.example.com mit den beiden Werten für den ersten Ressourceneintrag (192.0.2.9 und 192.0.2.10). In drei Viertel der Fälle (3/(1+3)) antwortet Amazon Route 53 auf Anfragen für www.example.com mit den beiden Werten für den zweiten Ressourceneintrag (192.0.2.11 und 192.0.2.12). Weitere

Informationen finden Sie in der Dokumentation zu Amazon Route 53 Mit dem Get-R53Change Cmdlet können Sie abfragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords = @()
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords = @()
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

Beispiel 4: Dieses Beispiel zeigt, wie gewichtete Alias-Ressourcendatensätze erstellt werden, vorausgesetzt, dass example.com die Domain ist, für die Sie gewichtete Alias-Ressourcendatensätze erstellen möchten. SetIdentifier unterscheidet die beiden gewichteten Alias-Ressourcendatensätze voneinander. Dieses Element ist erforderlich, da die Elemente „Name“ und „Type“ für beide Ressourceneintragsätze dieselben Werte haben. Z111111111111111 und Z3333333333333 sind Beispiele für gehostete Zonen

für den ELB-Load Balancer, angegeben durch den Wert von. IDs DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com und example-load-balancer -4444444444.us-east-1.elb.amazonaws.com sind Beispiele für Elastic Load Balancing Balancing-Domains, von denen Amazon Route 53 auf Anfragen für example.com antwortet. Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Sie können das Cmdlet verwenden, um abzufragen, wann die Änderungen Get-R53Change abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
```

```
}

Edit-R53ResourceRecordSet @params
```

Beispiel 5: In diesem Beispiel werden zwei Latenz-Alias-Ressourceneinträge erstellt, einer für einen ELB-Load Balancer in der Region US-West (Oregon) (us-west-2) und einer für einen Load Balancer in der Region Asien-Pazifik (Singapur) (ap-southeast-1). Weitere Informationen finden Sie in der Dokumentation zu Amazon Route 53 Mit dem Get-R53Change Cmdlet können Sie abfragen, wann die Änderungen abgeschlossen sind.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
```

```
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- Einzelheiten zur API finden Sie unter ChangeResourceRecordSets AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`CreateHostedZone`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `CreateHostedZone` verwendet wird.

CLI

AWS CLI

So erstellen Sie eine gehostete Zone

Mit dem folgenden `create-hosted-zone`-Befehl wird mithilfe der Aufruferreferenz `2014-04-01-18:47` eine gehostete Zone namens `example.com` hinzugefügt. Der optionale Kommentar enthält ein Leerzeichen und muss daher in Anführungszeichen gesetzt werden:

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Weitere Informationen finden Sie unter „Arbeiten mit gehosteten Zonen“ im Entwicklerhandbuch zu Amazon Route 53.

- Einzelheiten zur API finden Sie CreateHostedZonein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Erstellt eine neue gehostete Zone namens „example.com“, die mit einem wiederverwendbaren Delegationssatz verknüpft ist. Beachten Sie, dass Sie einen Wert für

den CallerReference Parameter angeben müssen, damit Anfragen, die bei Bedarf wiederholt werden müssen, ohne das Risiko eingehen zu müssen, dass der Vorgang zweimal ausgeführt wird. Da die gehostete Zone in einer VPC erstellt wird, ist sie automatisch privat und Sie sollten den PrivateZone Parameter - HostedZoneConfig _ nicht festlegen.

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Einzelheiten zur API finden Sie unter CreateHostedZone AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Erstellt eine neue gehostete Zone namens „example.com“, die mit einem wiederverwendbaren Delegationssatz verknüpft ist. Beachten Sie, dass Sie einen Wert für den CallerReference Parameter angeben müssen, damit Anfragen, die bei Bedarf wiederholt werden müssen, ohne das Risiko eingehen zu müssen, dass der Vorgang zweimal ausgeführt wird. Da die gehostete Zone in einer VPC erstellt wird, ist sie automatisch privat und Sie sollten den PrivateZone Parameter - HostedZoneConfig _ nicht festlegen.

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Einzelheiten zur API finden Sie unter CreateHostedZone AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DeleteHostedZone`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteHostedZone` verwendet wird.

CLI

AWS CLI

So löschen Sie eine gehostete Zone

Mit dem folgenden `delete-hosted-zone`-Befehl wird die gehostete Zone mit einer `id` von `Z36KTIQEXAMPLE` gelöscht:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Einzelheiten zur API finden Sie DeleteHostedZonein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Löscht die gehostete Zone mit der angegebenen ID. Sie werden zur Bestätigung aufgefordert, bevor der Befehl ausgeführt wird, es sei denn, Sie fügen den Schalterparameter -Force hinzu.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Einzelheiten zur API finden Sie unter DeleteHostedZone AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Löscht die gehostete Zone mit der angegebenen ID. Sie werden zur Bestätigung aufgefordert, bevor der Befehl ausgeführt wird, es sei denn, Sie fügen den Schalterparameter -Force hinzu.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Einzelheiten zur API finden Sie unter DeleteHostedZone AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetHostedZone`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetHostedZone` verwendet wird.

CLI

AWS CLI

So rufen Sie Informationen zu einer gehosteten Zone ab

Mit dem folgenden `get-hosted-zone`-Befehl werden Informationen über die gehostete Zone mit einem `id` von `Z1R8UBAEXAMPLE` abgerufen:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Einzelheiten zur API finden Sie GetHostedZonein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Gibt Details der gehosteten Zone mit der ID PJN98 FT9 Z1D633 zurück.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Einzelheiten zur API finden Sie unter AWS -Tools für PowerShell Cmdlet-Referenz (GetHostedZoneV4).

Tools für V5 PowerShell

Beispiel 1: Gibt Details der gehosteten Zone mit der ID PJN98 FT9 Z1D633 zurück.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Einzelheiten zur API finden Sie unter AWS -Tools für PowerShell Cmdlet-Referenz (GetHostedZoneV5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListHostedZones`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListHostedZones` verwendet wird.

CLI

AWS CLI

Um die Hosting-Zonen aufzulisten, die dem aktuellen AWS Konto zugeordnet sind

Der folgende `list-hosted-zones` Befehl listet zusammenfassende Informationen zu den ersten 100 Hostzonen auf, die dem aktuellen AWS Konto zugeordnet sind. :

```
aws route53 list-hosted-zones
```

Wenn Sie mehr als 100 gehostete Zonen haben oder wenn Sie sie in Gruppen von weniger als 100 auflisten möchten, fügen Sie den Parameter `--max-items` ein. Um zum Beispiel eine gehostete Zone nach der anderen aufzulisten, verwenden Sie den folgenden Befehl:

```
aws route53 list-hosted-zones --max-items 1
```

Um Informationen über die nächste gehostete Zone anzuzeigen, übernehmen Sie den Wert von `NextToken` aus der Antwort auf den vorherigen Befehl und fügen ihn in den Parameter `--starting-token` ein, zum Beispiel:

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Einzelheiten zur API finden Sie ListHostedZonesin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Gibt alle Ihre öffentlichen und privaten gehosteten Zonen aus.

```
Get-R53HostedZoneList
```

Beispiel 2: Gibt alle Hosting-Zonen aus, die dem wiederverwendbaren Delegierungssatz mit der ID NZ8 X2CISAMPLE zugeordnet sind

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Einzelheiten zur API finden Sie unter ListHostedZones AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Gibt alle Ihre öffentlichen und privaten gehosteten Zonen aus.

```
Get-R53HostedZoneList
```

Beispiel 2: Gibt alle Hosting-Zonen aus, die dem wiederverwendbaren Delegierungssatz mit der ID NZ8 X2CISAMPLE zugeordnet sind

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Einzelheiten zur API finden Sie unter ListHostedZones AWS -Tools für PowerShellCmdlet-Referenz (V5).

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
 aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!("  ID :   {}", zone_id);
        println!("  Name : {}", zone_name);
        println!();
    }

    Ok(())
}
```

- Einzelheiten zur API finden Sie ListHostedZonesin der API-Referenz zum AWS SDK für Rust.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`ListHostedZonesByName`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `ListHostedZonesByName` verwendet wird.

CLI

AWS CLI

Der folgende Befehl listet bis zu 100 gehostete Zonen auf, sortiert nach Domainnamen:

```
aws route53 list-hosted-zones-by-name
```

Ausgabe:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-2",
          "Config": {
              "Comment": "test2",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z119WBBTVP5WFX",
          "Name": "2.example.com."
      },
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
          "Name": "www.example.com."
      }
  ],
  "IsTruncated": false,
  "MaxItems": "100"
}
```

Der folgende Befehl listet die gehosteten Zonen nach Namen geordnet auf, beginnend mit `www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Ausgabe:

```
{
  "HostedZones": [
      {
```

```
            "ResourceRecordSetCount": 2,
            "CallerReference": "mwunderl20150527-1",
            "Config": {
                "Comment": "test",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "DNSName": "www.example.com",
    "IsTruncated": false,
    "MaxItems": "100"
}
```

- Einzelheiten zur API finden Sie ListHostedZonesByNamein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Gibt alle Ihre öffentlichen und privaten gehosteten Zonen in ASCII-Reihenfolge nach Domainnamen zurück.

```
Get-R53HostedZonesByName
```

Beispiel 2: Gibt Ihre öffentlichen und privaten gehosteten Zonen in ASCII-Reihenfolge nach Domainnamen zurück, beginnend mit dem angegebenen DNS-Namen.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Einzelheiten zur API finden Sie unter ListHostedZonesByName AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: Gibt alle Ihre öffentlichen und privaten gehosteten Zonen in ASCII-Reihenfolge nach Domainnamen zurück.

```
Get-R53HostedZonesByName
```

Beispiel 2: Gibt Ihre öffentlichen und privaten gehosteten Zonen in ASCII-Reihenfolge nach Domainnamen zurück, beginnend mit dem angegebenen DNS-Namen.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Einzelheiten zur API finden Sie unter ListHostedZonesByName AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`ListQueryLoggingConfigs`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `ListQueryLoggingConfigs` verwendet wird.

CLI

AWS CLI

So listen Sie die Konfigurationen zur Abfrageprotokollierung auf

Im folgenden `list-query-logging-configs` Beispiel werden Informationen zu den ersten 100 Konfigurationen für die Abfrageprotokollierung in Ihrem AWS Konto für die gehostete Zone aufgeführt`Z1OX3WQEXAMPLE`.

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

Ausgabe:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
```

```
}
```

Weitere Informationen finden Sie unter Protokollieren von DNS-Abfragen im Entwicklerhandbuch zu Amazon Route 53.

- Einzelheiten zur API finden Sie ListQueryLoggingConfigsunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden alle Konfigurationen für die DNS-Abfrageprotokollierung zurückgegeben, die mit dem aktuellen AWS-Konto verknüpft sind.

```
Get-R53QueryLoggingConfigList
```

Ausgabe:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   ------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- Einzelheiten zur API finden Sie unter ListQueryLoggingConfigs AWS -Tools für PowerShellCmdlet-Referenz (V4).

Tools für V5 PowerShell

Beispiel 1: In diesem Beispiel werden alle Konfigurationen für die DNS-Abfrageprotokollierung zurückgegeben, die mit dem aktuellen AWS-Konto verknüpft sind.

```
Get-R53QueryLoggingConfigList
```

Ausgabe:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
```

```
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- Einzelheiten zur API finden Sie unter ListQueryLoggingConfigs AWS -Tools für PowerShellCmdlet-Referenz (V5).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Route 53 mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele für die Route 53-Domainregistrierung mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Route 53-Domänenregistrierung mit einem AWS Software Development Kit (SDK) verwendet wird.

Bei Grundlagen handelt es sich um Codebeispiele, die Ihnen zeigen, wie Sie die wesentlichen Vorgänge innerhalb eines Services ausführen.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien anzeigen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Grundlegende Beispiele für die Route 53-Domainregistrierung mit AWS SDKs
  - Hallo Route-53-Domainregistrierung
  - Lernen Sie die Grundlagen der Route 53-Domainregistrierung mit einem AWS SDK kennen
  - Aktionen für die Route 53-Domänenregistrierung mit AWS SDKs

- Verwendung CheckDomainAvailability mit einem AWS SDK oder CLI
- Verwendung CheckDomainTransferability mit einem AWS SDK oder CLI
- Verwendung GetDomainDetail mit einem AWS SDK oder CLI
- Verwendung GetDomainSuggestions mit einem AWS SDK oder CLI
- Verwendung GetOperationDetail mit einem AWS SDK oder CLI
- Verwendung ListDomains mit einem AWS SDK oder CLI
- Verwendung ListOperations mit einem AWS SDK oder CLI
- ListPricesMit einem AWS SDK verwenden
- Verwendung RegisterDomain mit einem AWS SDK oder CLI
- Verwendung ViewBilling mit einem AWS SDK oder CLI

Grundlegende Beispiele für die Route 53-Domainregistrierung mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Grundlagen von Amazon Route 53 domain registration with verwendet AWS SDKs werden.

Beispiele

- Hallo Route-53-Domainregistrierung
- Lernen Sie die Grundlagen der Route 53-Domainregistrierung mit einem AWS SDK kennen
- Aktionen für die Route 53-Domänenregistrierung mit AWS SDKs
  - Verwendung CheckDomainAvailability mit einem AWS SDK oder CLI
  - Verwendung CheckDomainTransferability mit einem AWS SDK oder CLI
  - Verwendung GetDomainDetail mit einem AWS SDK oder CLI
  - Verwendung GetDomainSuggestions mit einem AWS SDK oder CLI
  - Verwendung GetOperationDetail mit einem AWS SDK oder CLI
  - Verwendung ListDomains mit einem AWS SDK oder CLI
  - Verwendung ListOperations mit einem AWS SDK oder CLI
  - ListPricesMit einem AWS SDK verwenden
  - Verwendung RegisterDomain mit einem AWS SDK oder CLI
  - Verwendung ViewBilling mit einem AWS SDK oder CLI

Hallo Route-53-Domainregistrierung

Die folgenden Codebeispiele zeigen, wie Sie mit der Verwendung der Route-53-Domainregistrierung beginnen.

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
```

```
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- Einzelheiten zur API finden Sie ListPricesin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
```

```
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
 String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
 route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
```

```
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
 pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
 + pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
 pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie ListPricesin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.
```

```
 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
```

```
            }
        }
    }
```

- Einzelheiten zur API finden Sie ListPricesin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Lernen Sie die Grundlagen der Route 53-Domainregistrierung mit einem AWS SDK kennen

Die folgenden Code-Beispiele veranschaulichen Folgendes:

- Auflisten der aktuellen Domains und der Vorgänge des letzten Jahres
- Anzeigen der Abrechnung für das vergangene Jahr und der Preise für Domaintypen
- Abrufen von Domainvorschlägen
- Überprüfen der Verfügbarkeit und Übertragbarkeit von Domains
- Optional: Anfordern einer Domainregistrierung
- Abrufen eines Vorgangsdetails
- Optional: Abrufen eines Domaindetails

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Führen Sie ein interaktives Szenario an einem Prompt aus.

```
public static class Route53DomainScenario
```

```
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.

    This .NET example performs the following tasks:
        1. List current domains.
        2. List operations in the past year.
        3. View billing for the account in the past year.
        4. View prices for domain types.
        5. Get domain suggestions.
        6. Check domain availability.
        7. Check domain transferability.
        8. Optionally, request a domain registration.
        9. Get an operation detail.
       10. Optionally, get a domain detail.
  */

    private static Route53Wrapper _route53Wrapper = null!;
    private static IConfiguration _configuration = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
                    .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonRoute53Domains>()
                .AddTransient<Route53Wrapper>()
            )
            .Build();

        _configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load settings from .json file.
            .AddJsonFile("settings.local.json",
                true) // Optionally, load local settings.
            .Build();
```

```
        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(Route53DomainScenario));

        _route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            await ListDomains();
            await ListOperations();
            await ListBillingRecords();
            await ListPrices();
            await ListDomainSuggestions();
            await CheckDomainAvailability();
            await CheckDomainTransferability();
            var operationId = await RequestDomainRegistration();
            await GetOperationalDetail(operationId);
            await GetDomainDetails();
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List account registered domains.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomains()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"1. List account domains.");
```

```
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {
            Console.WriteLine("\tNo domains found in this account.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain operations in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListOperations()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"2. List account domain operations in the past
year.");
        var operations = await _route53Wrapper.ListOperations(
            DateTime.Today.AddYears(-1));
        for (int i = 0; i < operations.Count; i++)
        {
            Console.WriteLine($"\tOperation Id: {operations[i].OperationId}");
            Console.WriteLine($"\tStatus: {operations[i].Status}");
            Console.WriteLine($"\tDate: {operations[i].SubmittedDate}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List billing in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListBillingRecords()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"3. View billing for the account in the past year.");
        var billingRecords = await _route53Wrapper.ViewBilling(
            DateTime.Today.AddYears(-1),
```

```
            DateTime.Today);
        for (int i = 0; i < billingRecords.Count; i++)
        {
            Console.WriteLine($"\tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
            Console.WriteLine($"\tOperation: {billingRecords[i].Operation}");
            Console.WriteLine($"\tPrice: {billingRecords[i].Price}");
        }
        if (!billingRecords.Any())
        {
            Console.WriteLine("\tNo billing records found in this account for the
past year.");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List prices for a few domain types.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListPrices()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. View prices for domain types.");
        var domainTypes = new List<string> { "net", "com", "org", "co" };

        var prices = await _route53Wrapper.ListPrices(domainTypes);
        foreach (var pr in prices)
        {
            Console.WriteLine($"\tName: {pr.Name}");
            Console.WriteLine($"\tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
            Console.WriteLine($"\tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
            Console.WriteLine($"\tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
            Console.WriteLine($"\tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
            Console.WriteLine();
        }
        Console.WriteLine(new string('-', 80));
    }
```

```
    /// <summary>
    /// List domain suggestions for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomainSuggestions()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"5. Get domain suggestions.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to get available domain
suggestions.");
            domainName = Console.ReadLine();
        }

        var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName,
true, 5);
        foreach (var suggestion in suggestions)
        {
            Console.WriteLine($"\tSuggestion Name: {suggestion.DomainName}");
            Console.WriteLine($"\tAvailability: {suggestion.Availability}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check availability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainAvailability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Check domain availability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
availability.");
            domainName = Console.ReadLine();
        }
```

```
        var availability = await
_route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\tAvailability: {availability}");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
_route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\tNote: This example uses domain request settings in
settings.json.");
        Console.WriteLine($"\tTo change the domain registration settings, set the
values in that file.");
        Console.WriteLine($"\tRemember, registering an actual domain will incur
an account billing cost.");
```

```
        Console.WriteLine($"\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();
            contact.CountryCode =
 CountryCode.FindValue(_configuration["Contact:CountryCode"]);
            contact.ContactType =
 ContactType.FindValue(_configuration["Contact:ContactType"]);

            _configuration.GetSection("Contact").Bind(contact);

            var operationId = await _route53Wrapper.RegisterDomain(
                domainName,
                Convert.ToBoolean(_configuration["AutoRenew"]),
                Convert.ToInt32(_configuration["DurationInYears"]),
                contact);
            if (operationId != null)
            {
                Console.WriteLine(
                    $"\tRegistration requested. Operation Id: {operationId}");
            }

            return operationId;
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }

    /// <summary>
    /// Get details for an operation.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task GetOperationalDetail(string? operationId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Get an operation detail.");

        var operationDetails =
            await _route53Wrapper.GetOperationDetail(operationId);
```

```
        Console.WriteLine(operationDetails);

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Optionally, get details for a registered domain.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\tNote: you must have a registered domain to get
 details.");
        Console.WriteLine($"\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }

            var domainDetails = await
 _route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}
```

Wrapper-Methoden, die vom Szenario für Route-53-Domainregistrierungsaktionen verwendet werden.

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
 ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }


    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
 ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }


    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
```

```
            }
        );
        return result.Availability.Value;
    }


    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }


    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
```

```
    }


    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
 {operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }


    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
```

```
   /// <param name="duration">The duration in years for the domain
registration.</param>
   /// <returns>The operation Id.</returns>
   public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
int duration, ContactDetail contact)
   {
       // This example uses the same contact information for admin, registrant,
and tech contacts.
       try
       {
           var result = await _amazonRoute53Domains.RegisterDomainAsync(
               new RegisterDomainRequest()
               {
                   AdminContact = contact,
                   RegistrantContact = contact,
                   TechContact = contact,
                   DomainName = domainName,
                   AutoRenew = autoRenew,
                   DurationInYears = duration,
                   PrivacyProtectAdminContact = false,
                   PrivacyProtectRegistrantContact = false,
                   PrivacyProtectTechContact = false
               }
           );
           return result.OperationId;
       }
       catch (InvalidInputException)
       {
           _logger.LogInformation($"Unable to request registration for domain
{domainName}");
           return null;
       }
   }


   /// <summary>
   /// View billing records for the account between a start and end date.
   /// </summary>
   /// <param name="startDate">The start date for billing results.</param>
   /// <param name="endDate">The end date for billing results.</param>
   /// <returns>A collection of billing records.</returns>
   public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
   {
```

```
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }


    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }


    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
```

```
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }


    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
 {result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der AWS SDK für .NET - API-Referenz.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
```

```
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
 *
 * This Java code example performs the following operations:
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
 * 4. View prices for domain types.
 * 5. Get domain suggestions.
 * 6. Check domain availability.
 * 7. Check domain transferability.
 * 8. Request a domain registration.
 * 9. Get operation details.
 * 10. Optionally, get domain details.
 */

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <domainType> <phoneNumber> <email> <domainSuggestion>
 <firstName> <lastName> <city>

                Where:
                    domainType - The domain type (for example, com).\s
                    phoneNumber - The phone number to use (for example,
 +91.9966564xxx)      email - The email address to use.      domainSuggestion -
 The domain suggestion (for example, findmy.accountants).\s
                    firstName - The first name to use to register a domain.\s
                    lastName -  The last name to use to register a domain.\s
                    city - the city to use to register a domain.\s
                    """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. List current domains.");
        listDomains(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. List operations in the past year.");
        listOperations(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. View billing for the account in the past year.");
        listBillingRecords(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. View prices for domain types.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Get domain suggestions.");
        listDomainSuggestions(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
domainSuggestion, phoneNumber, email, firstName,
                lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxx not found in xxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }

    public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
            System.out.println("The contact first name is " +
response.registrantContact().firstName());
```

```
            System.out.println("The contact last name is " +
response.registrantContact().lastName());
            System.out.println("The contact org name is " +
response.registrantContact().organizationName());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
        try {
            GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                    .operationId(operationId)
                    .build();

            GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
            System.out.println("Operation detail message is " +
response.message());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
            String domainSuggestion,
            String phoneNumber,
            String email,
            String firstName,
            String lastName,
            String city) {

        try {
            ContactDetail contactDetail = ContactDetail.builder()
                    .contactType(ContactType.COMPANY)
                    .state("LA")
                    .countryCode(CountryCode.IN)
```

```
                    .email(email)
                    .firstName(firstName)
                    .lastName(lastName)
                    .city(city)
                    .phoneNumber(phoneNumber)
                    .organizationName("My Org")
                    .addressLine1("My Address")
                    .zipCode("123 123")
                    .build();

            RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                    .adminContact(contactDetail)
                    .registrantContact(contactDetail)
                    .techContact(contactDetail)
                    .domainName(domainSuggestion)
                    .autoRenew(true)
                    .durationInYears(1)
                    .build();

            RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
            System.out.println("Registration requested. Operation Id: " +
response.operationId());
            return response.operationId();

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }

    public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainTransferabilityResponse response = route53DomainsClient
                    .checkDomainTransferability(transferabilityRequest);
            System.out.println("Transferability: " +
response.transferability().transferable().toString());
```

```
        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                    .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
```

```
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
                    .forEach(content -> System.out.println(" Name: " +
content.name() +
                            " Registration: " +
content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
                            " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            LocalDateTime localDateTime2 = localDateTime.minusYears(1);
            Instant myStartTime = localDateTime2.toInstant(zoneOffset);
            Instant myEndTime = localDateTime.toInstant(zoneOffset);
```

```
            ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                    .start(myStartTime)
                    .end(myEndTime)
                    .build();

            ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
            listRes.stream()
                    .flatMap(r -> r.billingRecords().stream())
                    .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                            " Operation: " + content.operationAsString() +
                            " Price: " + content.price()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
            Instant myTime = localDateTime.toInstant(zoneOffset);

            ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));
```

```
        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der AWS SDK for Java 2.x - API-Referenz.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
 */

val DASHES: String = String(CharArray(80)).replace("\u0000", "-")

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
 <lastName> <city>
        Where:
           domainType - The domain type (for example, com).
```

```
            phoneNumber - The phone number to use (for example, +1.2065550100)

            email - The email address to use.
            domainSuggestion - The domain suggestion (for example,
    findmy.example).
            firstName - The first name to use to register a domain.
            lastName -  The last name to use to register a domain.
            city - The city to use to register a domain.
       """

       if (args.size != 7) {
           println(usage)
           exitProcess(1)
       }

       val domainType = args[0]
       val phoneNumber = args[1]
       val email = args[2]
       val domainSuggestion = args[3]
       val firstName = args[4]
       val lastName = args[5]
       val city = args[6]

       println(DASHES)
       println("Welcome to the Amazon Route 53 domains example scenario.")
       println(DASHES)

       println(DASHES)
       println("1. List current domains.")
       listDomains()
       println(DASHES)

       println(DASHES)
       println("2. List operations in the past year.")
       listOperations()
       println(DASHES)

       println(DASHES)
       println("3. View billing for the account in the past year.")
       listBillingRecords()
       println(DASHES)

       println(DASHES)
       println("4. View prices for domain types.")
```

```
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("7. Check domain transferability.")
    checkDomainTransferability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("8. Request a domain registration.")
    val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
 firstName, lastName, city)
    println(DASHES)

    println(DASHES)
    println("9. Get operation details.")
    getOperationalDetail(opId)
    println(DASHES)

    println(DASHES)
    println("10. Get domain details.")
    println("Note: You must have a registered domain to get details.")
    println("Otherwise an exception is thrown that states ")
    println("Domain xxxxxxx not found in xxxxxxx account.")
    getDomainDetails(domainSuggestion)
    println(DASHES)
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
```

```
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
```

```
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
```

```
    }
}

suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
```

```
}

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }
```

```
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}

suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Kotlin.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Aktionen für die Route 53-Domänenregistrierung mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Route 53-Domänenregistrierungsaktionen mit ausgeführt AWS SDKs werden. Jedes Beispiel enthält einen Link zu GitHub, über den Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der Amazon Route 53 domain registration -API-Referenz.

Beispiele

- Verwendung CheckDomainAvailability mit einem AWS SDK oder CLI
- Verwendung CheckDomainTransferability mit einem AWS SDK oder CLI
- Verwendung GetDomainDetail mit einem AWS SDK oder CLI
- Verwendung GetDomainSuggestions mit einem AWS SDK oder CLI
- Verwendung GetOperationDetail mit einem AWS SDK oder CLI
- Verwendung ListDomains mit einem AWS SDK oder CLI
- Verwendung ListOperations mit einem AWS SDK oder CLI
- ListPricesMit einem AWS SDK verwenden
- Verwendung RegisterDomain mit einem AWS SDK oder CLI
- Verwendung ViewBilling mit einem AWS SDK oder CLI

Verwendung **`CheckDomainAvailability`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `CheckDomainAvailability` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- Einzelheiten zur API finden Sie CheckDomainAvailabilityin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So stellen Sie fest, ob Sie einen Domainnamen mit Route 53 registrieren können

Der folgende `check-domain-availability`-Befehl gibt Informationen darüber zurück, ob der Domainname `example.com` für die Registrierung über Route 53 verfügbar ist.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

Ausgabe:

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 unterstützt eine große Anzahl von Top-Level-Domains (TLDs), z. B. `.com` und `.jp`, aber wir unterstützen nicht alle verfügbaren TLDs Domains. Wenn Sie die Verfügbarkeit einer Domain überprüfen und Route 53 die TLD nicht unterstützt, gibt `check-domain-availability` die folgende Meldung zurück.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Eine Liste der Domains TLDs , die Sie bei der Registrierung einer Domain bei Route 53 verwenden können, finden Sie unter Domains, die Sie bei Amazon Route 53 registrieren können im Amazon Route 53 53-Entwicklerhandbuch. Weitere Informationen zum Registrieren einer Domain mit Route 53 finden Sie unter Registrieren einer neuen Domain im Entwicklerhandbuch für Amazon Route 53.

- Einzelheiten zur API finden Sie CheckDomainAvailabilityin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainAvailabilityResponse response = route53DomainsClient
                   .checkDomainAvailability(availabilityRequest);
           System.out.println(domainSuggestion + " is " +
response.availability().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie CheckDomainAvailabilityin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
{ route53DomainsClient ->
```

```
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
}
```

- Einzelheiten zur API finden Sie CheckDomainAvailabilityin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CheckDomainTransferability`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `CheckDomainTransferability` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
```

```
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }
```

- Einzelheiten zur API finden Sie CheckDomainTransferabilityin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So stellen Sie fest, ob eine Domain auf Route 53 übertragen werden kann 53

Der folgende `check-domain-transferability`-Befehl gibt Informationen darüber zurück, ob Sie den Domainnamen `example.com` auf Route 53 übertragen können.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Ausgabe:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

Weitere Informationen finden Sie unter Übertragen der Registrierung für eine Domain an Amazon Route 53 im Entwicklerhandbuch für Amazon Route 53.

- Einzelheiten zur API finden Sie CheckDomainTransferabilityin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
           System.out.println("Transferability: " +
response.transferability().transferable().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie CheckDomainTransferabilityin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- Einzelheiten zur API finden Sie CheckDomainTransferabilityin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetDomainDetail`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `GetDomainDetail` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
{result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
```

- Einzelheiten zur API finden Sie GetDomainDetailin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So rufen Sie detaillierte Informationen zu einer bestimmten Domain ab

Der folgende `get-domain-detail`-Befehl zeigt detaillierte Informationen über die angegebene Domain an.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

Ausgabe:

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
```

```
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon",
    "RegistrarUrl": "http://registrar.amazon.com",
```

```
    "AbuseContactEmail": "abuse@registrar.amazon.com",
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- Einzelheiten zur API finden Sie GetDomainDetailin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
```

```
    }
```

- Einzelheiten zur API finden Sie GetDomainDetailin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}
```

- Einzelheiten zur API finden Sie GetDomainDetailin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetDomainSuggestions`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `GetDomainSuggestions` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }
```

- Einzelheiten zur API finden Sie GetDomainSuggestionsin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So rufen Sie eine Liste der vorgeschlagenen Domainnamen ab

Der folgende `get-domain-suggestions`-Befehl zeigt eine Liste mit vorgeschlagenen Domainnamen an, die auf dem Domainnamen `example.com` basieren. Die Antwort enthält nur verfügbare Domainnamen. Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

Ausgabe:

```
{
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
```

```
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
       },
        {
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- Einzelheiten zur API finden Sie GetDomainSuggestionsin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                   .domainName(domainSuggestion)
```

```
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie GetDomainSuggestionsin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
```

```
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}
```

- Einzelheiten zur API finden Sie GetDomainSuggestionsin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetOperationDetail`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `GetOperationDetail` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }
```

- Einzelheiten zur API finden Sie GetOperationDetailin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So rufen Sie den aktuellen Status einer Operation ab

Einige Domainregistrierungsvorgänge werden asynchron ausgeführt und geben eine Antwort zurück, bevor sie abgeschlossen sind. Diese Operationen geben eine Vorgangs-ID zurück, mit der Sie den aktuellen Status abrufen können. Der folgende `get-operation-detail`-Befehl gibt den Status des angegebenen Vorgangs zurück.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Ausgabe:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- Einzelheiten zur API finden Sie GetOperationDetailin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
```

```
                    .operationId(operationId)
                    .build();

            GetOperationDetailResponse response =
 route53DomainsClient.getOperationDetail(detailRequest);
            System.out.println("Operation detail message is " +
 response.message());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie GetOperationDetailin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- Einzelheiten zur API finden Sie GetOperationDetailin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListDomains`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListDomains` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
```

```
            results.Add(domain);
        }
        return results;
    }
```

- Einzelheiten zur API finden Sie ListDomainsin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

Um die Domains aufzulisten, die mit dem aktuellen AWS Konto registriert sind

Der folgende `list-domains` Befehl listet zusammenfassende Informationen zu den Domänen auf, die mit dem aktuellen AWS Konto registriert sind.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains list-domains
    --region us-east-1
```

Ausgabe:

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
```

```
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- Einzelheiten zur API finden Sie ListDomainsunter AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie ListDomainsin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listDomains() {
    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- Einzelheiten zur API finden Sie ListDomainsin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListOperations`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ListOperations` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }
```

- Einzelheiten zur API finden Sie ListOperationsin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So listen Sie den Status von Vorgängen auf, die eine Vorgangs-ID zurückgeben

Einige Domainregistrierungsvorgänge werden asynchron ausgeführt und geben eine Antwort zurück, bevor sie abgeschlossen sind. Diese Operationen geben eine Vorgangs-ID zurück, mit der Sie den aktuellen Status abrufen können. Der folgende `list-operations`-Befehl listet zusammenfassende Informationen, einschließlich des Status, zu den aktuellen Domainregistrierungsvorgängen auf.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains list-operations
    --region us-east-1
```

Ausgabe:

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

Die Ausgabe umfasst alle Operationen, die eine Vorgangs-ID zurückgeben und die Sie für alle Domains ausgeführt haben, die Sie jemals mit dem AWS Girokonto registriert haben. Wenn Sie nur die Operationen abrufen möchten, die Sie nach einem bestimmten Datum eingereicht haben, können Sie den `submitted-since`-Parameter einbeziehen und ein Datum im Unix-Format und in koordinierter Weltzeit (UTC) angeben. Der folgende Befehl ruft den Status aller Operationen ab, die am 1. Januar 2020 nach 12:00 Uhr UTC gesendet wurden.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- Einzelheiten zur API finden Sie ListOperationsin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void listOperations(Route53DomainsClient route53DomainsClient)
{
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           localDateTime = localDateTime.minusYears(1);
           Instant myTime = localDateTime.toInstant(zoneOffset);

           ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
                   .submittedSince(myTime)
                   .build();

           ListOperationsIterable listRes =
route53DomainsClient.listOperationsPaginator(operationsRequest);
           listRes.stream()
```

```
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
 content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie ListOperationsin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
```

```
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}
```

- Einzelheiten zur API finden Sie ListOperationsin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

`ListPrices`Mit einem AWS SDK verwenden

Die folgenden Code-Beispiele zeigen, wie `ListPrices` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
```

```
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

- Einzelheiten zur API finden Sie ListPricesin der AWS SDK für .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
                    .forEach(content -> System.out.println(" Name: " +
content.name() +
                            " Registration: " +
content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
```

```
                            " Renewal: " + content.renewalPrice().price() + " " +
 content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Einzelheiten zur API finden Sie ListPricesin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
```

```
            }
    }
}
```

- Einzelheiten zur API finden Sie ListPricesin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`RegisterDomain`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `RegisterDomain` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
```

```
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }
```

- Einzelheiten zur API finden Sie RegisterDomainin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

So registrieren Sie eine Domain

Der folgende `register-domain`-Befehl registriert eine Domain und ruft alle Parameterwerte aus einer Datei im JSON-Format ab.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

Inhalt von `register-domain.json`:

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
```

```
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

Ausgabe:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Sie können `get-operation-detail` ausführen, um zu bestätigen, dass der Vorgang erfolgreich war. Weitere Informationen finden Sie unter get-operation-detail.

Weitere Informationen finden Sie unter Registrieren einer neuen Domain im Entwicklerhandbuch zu Amazon Route 53.

Informationen darüber, für welche Top-Level-Domains (TLDs) Werte erforderlich sind `ExtraParams` und welche Werte gültig sind, finden Sie ExtraParamin der Amazon Route 53 API-Referenz.

- Einzelheiten zur API finden Sie RegisterDomainin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
           String domainSuggestion,
           String phoneNumber,
           String email,
           String firstName,
           String lastName,
           String city) {

       try {
           ContactDetail contactDetail = ContactDetail.builder()
                   .contactType(ContactType.COMPANY)
                   .state("LA")
                   .countryCode(CountryCode.IN)
                   .email(email)
                   .firstName(firstName)
                   .lastName(lastName)
                   .city(city)
                   .phoneNumber(phoneNumber)
                   .organizationName("My Org")
                   .addressLine1("My Address")
                   .zipCode("123 123")
                   .build();

           RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                   .adminContact(contactDetail)
                   .registrantContact(contactDetail)
                   .techContact(contactDetail)
                   .domainName(domainSuggestion)
                   .autoRenew(true)
                   .durationInYears(1)
                   .build();

           RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
           System.out.println("Registration requested. Operation Id: " +
response.operationId());
           return response.operationId();

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
```

```
        return "";
    }
```

- Einzelheiten zur API finden Sie RegisterDomainin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
```

```
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- Einzelheiten zur API finden Sie RegisterDomainin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ViewBilling`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `ViewBilling` verwendet wird.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Kennenlernen der Grundlagen

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }
```

- Einzelheiten zur API finden Sie ViewBillingin der AWS SDK für .NET API-Referenz.

CLI

AWS CLI

Um Abrechnungsinformationen für die Gebühren für die Domainregistrierung für das AWS Girokonto zu erhalten

Mit dem folgenden `view-billing`-Befehl werden alle domainbezogenen Abrechnungsdatensätze für das aktuelle Konto für den Zeitraum vom 1. Januar 2018 (1514764800 in Unix-Zeit) bis Mitternacht am 31. Dezember 2019 (1577836800 in Unix-Zeit) zurückgegeben.

Dieser Befehl wird nur in der `us-east-1`-Region ausgeführt. Wenn Ihre Standardregion auf `us-east-1` gesetzt ist, können Sie den `region`-Parameter weglassen.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

Ausgabe:

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
}
```

Weitere Informationen finden Sie ViewBillingin der Amazon Route 53 API-Referenz.

- Einzelheiten zur API finden Sie ViewBillingunter AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();

           ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
           listRes.stream()
                   .flatMap(r -> r.billingRecords().stream())
                   .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                           " Operation: " + content.operationAsString() +
                           " Price: " + content.price()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Einzelheiten zur API finden Sie ViewBillingin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient.fromEnvironment { region = "us-east-1" }.use
 { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}
```

- Einzelheiten zur API finden Sie ViewBillingin der API-Referenz zum AWS SDK für Kotlin.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterRoute 53 mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Sicherheit in Amazon Route 53.

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den für Amazon Route 53 geltenden Compliance-Programmen finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS -Services.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Route 53 zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Route 53 zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Ihnen bei der Überwachung und Sicherung Ihrer Route 53-Ressourcen helfen.

Topics

Datenschutz in der Route 53

Das AWS Modell der mit gilt für den Datenschutz in Amazon Route 53. Wie in diesem Modell beschrieben, AWS ist es verantwortlich für den Schutz der globalen Infrastruktur, auf der die gesamte Infrastruktur läuft AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Route 53 oder anderen Geräten arbeiten und dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Schutz vor hängenden Delegierungsdatensätzen in Route 53

Mit Route 53 kann ein Kunde eine gehostete Zone erstellen, um beispielsweise `example.com` seine DNS-Einträge zu hosten. Jede gehostete Zone verfügt über einen „Delegierungssatz“, der aus vier Nameservern besteht, die ein Kunde zur Konfiguration von NS-Einträgen in der übergeordneten Domain verwenden kann. Diese NS-Einträge können als „Delegations-NS-Einträge“ oder „Delegationsdatensätze“ bezeichnet werden.

Damit die gehostete `example.com` Route 53 53-Zone autoritativ wird, muss der rechtmäßige Eigentümer der `example.com` Domain Delegierungseinträge in seiner übergeordneten Domain „.com“ über den Domain-Registrar konfigurieren. In Fällen, in denen ein Kunde den Zugriff auf die vier in der übergeordneten Domain konfigurierten Nameserver verliert, z. B. weil die zugehörige Hosting-Zone gelöscht wurde, kann dies ein Risiko darstellen, das ein Angreifer ausnutzen kann. Dieses Risiko wird als „hängengebliebene Delegationsdaten“ bezeichnet.

Route 53 schützt vor dem Risiko eines hängenden Delegierungsdatensatzes für den Fall, dass eine gehostete Zone gelöscht wird. Wenn nach dem Löschen eine neue gehostete Zone mit demselben Domänennamen erstellt wird, überprüft Route 53, ob die Delegierungseinträge, die auf die gelöschte Hosting-Zone verweisen, noch in der übergeordneten Domäne vorhanden sind. Wenn dies der Fall ist, verhindert Route 53, dass sich überschneidende Nameserver zugewiesen werden. Dies ist Szenario 1 in den folgenden Beispielen.

Es gibt jedoch noch andere Risiken im Zusammenhang mit Delegierungsaufzeichnungen, vor denen Route 53 nicht schützen kann, wie in den folgenden Beispielen in den Szenarien 2 und 3 beschrieben. Um sich vor diesen umfassenderen Risiken zu schützen, stellen Sie sicher, dass die übergeordneten NS-Einträge mit dem Delegierungssatz für die gehostete Route 53-Zone übereinstimmen. Sie finden den Delegierungssatz einer Hosting-Zone über die Route 53-Konsole oder AWS CLI. Für weitere Informationen siehe Auflisten von Datensätzen oder get-hosted-zone.

Darüber hinaus kann die Aktivierung der DNSSEC-Signatur für eine gehostete Route 53 53-Zone als weitere Schutzebene dienen, die über die oben genannten bewährten Methoden hinausgeht. DNSSEC authentifiziert, dass DNS-Antworten von der autoritativen Quelle stammen, und schützt so effektiv vor diesem Risiko. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

Beispiele

In den folgenden Beispielen gehen wir davon aus, dass Sie über eine Domain und deren untergeordnete Domain `example.com` verfügen. `child.example.com` Wir werden erklären, wie in verschiedenen Szenarien fehlerhafte Delegierungsdatensätze erstellt werden können, wie Route 53 Ihre Domain vor Missbrauch schützt und wie Sie die Risiken, die mit unbrauchbaren Delegierungsdatensätzen verbunden sind, wirksam mindern können.

Szenario 1:

<ns3><ns4>Sie erstellen eine gehostete Zone `child.example.com` mit vier Nameservern:<ns1>,<ns2>, und. Sie richten die Delegierung in der Hosting-Zone `example.com` ordnungsgemäß ein und erstellen Delegierungs-NS-Einträge für `child.example.com` vier Nameserver <ns1><ns2>,<ns3>, und<ns4>. Wenn die `child.example.com` gehostete Zone gelöscht wird, ohne dass die Delegierungs-NS-Einträge entfernt werden`example.com`, schützt Route 53 vor `child.example.com` dem Risiko der Übertragung von Delegierungseinträgen <ns1><ns2><ns3>, indem verhindert wird,, und dass <ns4>neu erstellten Hosting-Zonen mit demselben Domainnamen zugewiesen werden.

Szenario 2:

Ähnlich wie in Szenario 1, aber dieses Mal löschen Sie die untergeordnete gehostete Zone UND die DNS-Einträge der Delegierung in der Hosting-Zone`example.com`. Sie fügen jedoch die Delegations-NS-Einträge<ns1>,, <ns2><ns3>und wieder hinzu, <ns4>ohne eine untergeordnete gehostete Zone zu erstellen. In diesem Fall <ns1><ns2><ns3><ns4>handelt es sich bei,, und um Delegierungsdatensätze, da Route 53 den Hold aufhebt, der die <ns1><ns2><ns3><ns4>Zuweisung von,, und verhindert hat, und ermöglicht nun neu erstellten Hosting-Zonen die Verwendung der oben genannten Nameserver. Um das Risiko zu minimieren, entfernen Sie, <ns1><ns2><ns3>, und <ns4>aus den Delegierungsdatensätzen und fügen Sie sie erst wieder hinzu, wenn die untergeordnete gehostete Zone erstellt wurde.

Szenario 3:

<ns4>In diesem Szenario erstellen Sie einen wiederverwendbaren Route 53-Delegierungssatz mit den Nameservern <ns1><ns2>,<ns3>, und. Anschließend delegieren Sie die Domäne `example.com` an diese Nameserver in der übergeordneten Domäne`.com`. Sie haben die Hosting-Zone für `example.com` jedoch noch nicht im wiederverwendbaren Delegierungssatz erstellt. Hier, <ns1><ns2><ns3>, und hängen <ns4>die Delegierungsdatensätze. <ns4>Um das Risiko zu minimieren, erstellen Sie die Hosting-Zone mithilfe des wiederverwendbaren Delegierungssatzes mit den Nameservern<ns1>, <ns2><ns3>, und.

Identity and Access Management in Amazon Route 53

Um Vorgänge auf Amazon Route 53-Ressourcen ausführen zu können, z. B. die Registrierung einer Domain oder die Aktualisierung eines Datensatzes AWS Identity and Access Management (IAM), müssen Sie authentifizieren, dass Sie ein zugelassener AWS Benutzer sind. Wenn Sie die Route-53-Konsole verwenden, authentifizieren Sie Ihre Identität durch Angabe Ihres AWS -Benutzernamens und des zugehörigen Passworts.

Nachdem Sie Ihre Identität authentifiziert haben, kontrolliert IAM Ihren Zugriff auf, AWS indem es überprüft, ob Sie über die erforderlichen Berechtigungen zur Durchführung von Vorgängen und zum Zugriff auf Ressourcen verfügen. Wenn Sie ein Kontoadministrator sind, können Sie mithilfe von IAM den Zugriff anderer Benutzer auf die mit Ihrem Konto verknüpften Ressourcen steuern.

In diesem Abschnitt wird erläutert, wie Sie IAM und Route 53 verwenden, um Ihre Ressourcen zu schützen.

Themen

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden

finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln oder indem Sie eine AWS Oder-API-Operation AWS CLI aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Zugriffskontrolle

Um Amazon-Route-53-Ressourcen zu erstellen, zu aktualisieren, zu löschen oder zu aktualisieren, benötigten Sie die Berechtigungen zum Ausführen der Operation sowie die Berechtigung für den Zugriff auf die entsprechenden Ressourcen.

In den folgenden Abschnitten wird die Verwaltung von Berechtigungen für Route 53 beschrieben. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Route-53-Ressourcen

Jede AWS Ressource gehört einem AWS Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf eine Ressource werden durch Berechtigungsrichtlinien geregelt.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen über Administratoren finden Sie unter Bewährte Methoden für IAM im IAM Benutzerhandbuch.

Wenn Sie Berechtigungen erteilen, entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen Berechtigungen vergeben werden und welche Aktionen für die Benutzer zulässig sind.

Benutzer benötigen programmgesteuerten Zugriff, wenn sie mit AWS außerhalb von interagieren möchten. AWS-Managementkonsole Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldeinformationen als temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zum AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command Line Interface Benutzerhandbuch. • Weitere Informationen finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. AWS SDKs
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		• Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Ref erenzhandbuch.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldeinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Themen

- ARNs für Amazon Route 53-Ressourcen
- Grundlegendes zum Eigentum an Ressourcen
- Verwaltung des Zugriffs auf -Ressourcen
- Angeben der Richtlinienelemente: Ressourcen, Aktionen, Effekte und Prinzipale
- Angeben von Bedingungen in einer Richtlinie

ARNs für Amazon Route 53-Ressourcen

Amazon Route 53 unterstützt eine Vielzahl von Ressourcentypen für DNS, die Zustandsprüfung und die Domainregistrierung. In einer Richtlinie können Sie den Zugriff auf die folgenden Ressourcen gewähren oder verweigern, indem Sie * für den ARN verwenden:

- Health checks (Zustandsprüfungen)
- Gehostete Zonen
- Wiederverwendbare Delegationssätze
- Status eines Ressourcendatensatz-Änderungsstapels (nur API)
- Datenverkehrsrichtlinien (Datenfluss)
- Datenverkehrsrichtlinien-Instances (Datenfluss)

Nicht alle Route-53-Ressourcen unterstützen Berechtigungen. Für die folgenden Ressourcen können Sie keinen Zugriff gewähren oder verweigern:

- Domains
- Individuelle Datensätze
- Tags für Domänen
- Tags für Zustandsprüfungen
- Tags für gehostete Zonen

Route 53 stellt API-Aktionen für die Arbeit mit diesen verschiedenen Typen von Ressourcen bereit. Weitere Informationen finden Sie unter Amazon Route 53 API Reference. Eine Liste der Aktionen mit den anzugebenden ARNs, mit denen ihnen Berechtigungen erteilt oder entzogen werden, finden Sie unter Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

Grundlegendes zum Eigentum an Ressourcen

Ein AWS Konto besitzt die Ressourcen, die in dem Konto erstellt wurden, unabhängig davon, wer die Ressourcen erstellt hat. Insbesondere ist der Ressourcenbesitzer das AWS Konto der Prinzipalentität (d. h. das Stammkonto oder eine IAM-Rolle), das die Anfrage zur Ressourcenerstellung authentifiziert.

Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Root-Kontoanmeldeinformationen Ihres AWS Kontos verwenden, um eine gehostete Zone zu erstellen, ist Ihr AWS Konto der Eigentümer der Ressource.
- Wenn Sie in Ihrem AWS Konto einen Benutzer erstellen und diesem Benutzer Berechtigungen zum Erstellen einer gehosteten Zone gewähren, kann der Benutzer eine gehostete Zone erstellen. Eigentümer der gehosteten Zone ist jedoch das AWS -Konto, zu dem der Benutzer gehört.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Erstellen einer gehosteten Zone erstellen, kann jeder, der diese Rolle übernehmen kann, eine gehostete Zone erstellen. Ihr AWS Konto, zu dem die Rolle gehört, besitzt die gehostete Zonenressource.

Verwaltung des Zugriffs auf -Ressourcen

Eine Berechtigungsrichtlinie gibt an, wer Zugriff auf welche Objekte hat. In diesem Abschnitt werden die Optionen zum Erstellen von Berechtigungsrichtlinien für Amazon Route 53 erläutert. Allgemeine Informationen über die Syntax und Beschreibungen von IAM-Richtlinien finden Sie in der AWS IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die einer IAM-Identität zugeordnet sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, während Richtlinien, die einer Ressource zugeordnet sind, als ressourcenbasierte Richtlinien bezeichnet werden. Route 53 unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Identitätsbasierte Richtlinien (IAM-Richtlinien)
- Ressourcenbasierte Richtlinien

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Berechtigungsrichtlinien Benutzern oder Gruppen in Ihrem Konto zuweisen – Ein Kontoadministrator kann eine Berechtigungsrichtlinie verwenden, die einem bestimmten Benutzer zugeordnet ist, um diesem Benutzer Berechtigungen zum Erstellen von Amazon-Route-53-Ressourcen zu erteilen.
- Einer Rolle eine Berechtigungsrichtlinie zuordnen (kontoübergreifende Berechtigungen gewähren) — Sie können einem Benutzer, der mit einem anderen AWS Konto erstellt wurde, die Erlaubnis zur Durchführung von Route 53-Aktionen erteilen. Dazu ordnen Sie einer IAM-Rolle eine

Berechtigungsrichtlinie zu und erlauben dann dem Benutzer in dem anderen Konto, die Rolle einzunehmen. Im folgenden Beispiel wird erklärt, wie dieser Vorgang für zwei AWS -Konten, Konto A und Konto B, funktioniert:

1. Der Administrator von Konto A erstellt eine IAM-Rolle und weist ihr eine Berechtigungsrichtlinie zu, die Berechtigungen zum Erstellen von oder für den Zugriff auf Ressourcen erteilt, die Konto A gehören.
2. Der Administrator von Konto A weist der Rolle eine Vertrauensrichtlinie zu. Die Vertrauensrichtlinie identifiziert Konto B als Prinzipal, der die Rolle einnehmen darf.
3. Anschließend kann der Administrator von Konto B Berechtigungen für Benutzer oder Gruppen in Konto B zuweisen, sodass diese die Rolle einnehmen können. Auf diese Weise können Benutzer in Konto B Ressourcen in Konto A erstellen bzw. darauf zugreifen.

Weitere Informationen zum Delegieren von Berechtigungen an Benutzer in einem anderen AWS Konto finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie ermöglicht es einem Benutzer, die Aktion `CreateHostedZone` auszuführen und eine öffentliche gehostete Zone für ein AWS -Konto zu erstellen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Wenn Sie möchten, dass die Richtlinie auch für privat gehostete Zonen gilt, müssen Sie die Berechtigungen zur Verwendung der Route `AssociateVPCWithHostedZone` 53-Aktion und zweier EC2 Amazon-Aktionen gewähren, `DescribeVpcs` und`DescribeRegion`, wie im folgenden Beispiel gezeigt,:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zum Zuweisen von Richtlinien zu Identitäten für Route 53 finden Sie unter Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Route 53. Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon S3, unterstützen auch die Zuordnung von Berechtigungsrichtlinien zu Ressourcen. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. Amazon Route 53 unterstützt nicht das Anfügen von Richtlinien an Ressourcen.

Angeben der Richtlinienelemente: Ressourcen, Aktionen, Effekte und Prinzipale

Amazon Route 53 enthält API-Aktionen (siehe Amazon-Route-53-API-Referenz), die Sie für jede Route-53-Ressource verwenden können (siehe ARNs für Amazon Route 53-Ressourcen). Sie

können Benutzern oder verbundenen Benutzern Berechtigungen zur Durchführung beliebiger oder aller dieser Aktionen erteilen. Beachten Sie, dass einige API-Aktionen, z. B. die Registrierung einer Domäne, Berechtigungen zur Durchführung mehrerer Aktionen erfordern.

Grundlegende Richtlinienelemente:

- Ressource – Sie verwenden einen Amazon-Ressourcennamen (ARN), um die Ressource, für welche die Richtlinie gilt, zu identifizieren. Weitere Informationen finden Sie unter ARNs für Amazon Route 53-Ressourcen.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Beispiel: Abhängig von dem angegebenen `Effect` erlaubt oder verweigert die Berechtigung `route53:CreateHostedZone` Benutzern die Durchführung der Route-53-Aktion `CreateHostedZone`.
- Effekt – Dies ist die von Ihnen festgelegte Auswirkung (entweder Zugriffserlaubnis oder Zugriffsverweigerung), wenn ein Benutzer versucht, die jeweilige Aktion für die angegebene Ressource durchzuführen. Wenn Sie den Zugriff auf eine Aktion nicht ausdrücklich gestatten, wird er implizit verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). Route 53 unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen über die Syntax und Beschreibungen von IAM-Richtlinien finden Sie in der AWS IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine mit einer Liste von allen Route-53-API-Operationen und den Ressourcen, für welche diese gelten, finden Sie unter Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der IAM-Richtliniensyntax die Bedingungen angeben, unter denen die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben

von Bedingungen in der Sprache der Richtlinie finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für Route 53 gibt es keine speziellen Bedingungsschlüssel. Es gibt jedoch AWS zahlreiche Bedingungsschlüssel, die Sie nach Bedarf verwenden können. Eine vollständige Liste der AWS Wide Keys finden Sie unter Verfügbare Schlüssel für Bedingungen im IAM-Benutzerhandbuch.

Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Route 53

Dieses Thema stellt Beispiele für identitätsbasierte Richtlinien bereit, die zeigen, wie ein Kontoadministrator Berechtigungsrichtlinien an IAM-Identitäten anfügen und damit Berechtigungen für die Durchführung von Operationen für Amazon-Route-53-Ressourcen gewähren kann.

Important

Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die Grundkonzepte und Optionen zum Verwalten des Zugriffs auf Ihre Route-53-Ressourcen erläutert werden. Weitere Informationen finden Sie unter Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Route-53-Ressourcen.

Note

Wenn Zugriff gewährt wird, müssen die gehostete Zone und die Amazon VPC zur selben Partition gehören. Eine Partition ist eine Gruppe von. AWS-Regionen Jede AWS-Konto ist auf eine Partition beschränkt.
Im Folgenden werden die unterstützten Partitionen angezeigt:

- `aws` - AWS-Regionen
- `aws-cn` – Chinesiche Regionen
- `aws-us-gov` - AWS GovCloud (US) Region

Weitere Informationen finden Sie unter Zugriffsverwaltung und Amazon-Route-53-Endpunkte und Kontingente in der Allgemeinen Referenz zu AWS .

Themen

- Erforderliche Berechtigungen zur Verwendung der Amazon-Route-53-Konsole
- Beispielberechtigungen für einen Domänendatensatzbesitzer
- Route 53 vom Kunden verwaltete Schlüsselberechtigungen für DNSSEC-Signierung erforderlich
- Beispiele für vom Kunden verwaltete Richtlinien

Das folgende Beispiel zeigt eine Berechtigungsrichtlinie. Der Abschnitt `Sid` (die Anweisungs-ID) ist optional:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid" : "AllowPublicHostedZonePermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:UpdateHostedZoneComment",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:DeleteHostedZone",
                "route53:ChangeResourceRecordSets",
                "route53:ListResourceRecordSets",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZonesByName"
            ],
            "Resource": "*"
        },
        {
         "Sid" : "AllowHealthCheckPermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHealthCheck",
                "route53:UpdateHealthCheck",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:DeleteHealthCheck",
                "route53:GetCheckerIpRanges",
```

```
                "route53:GetHealthCheckCount",
                "route53:GetHealthCheckStatus",
                "route53:GetHealthCheckLastFailureReason"
            ],
            "Resource": "*"
        }
    ]
}
```

Die Richtlinie enthält zwei Anweisungen:

- Die erste Anweisung gewährt Berechtigungen für die Aktionen, die zum Erstellen und Verwalten von öffentlichen gehosteten Zonen und deren Datensätzen erforderlich sind. Das Platzhalterzeichen (*) im Amazon-Ressourcennamen (ARN) gewährt Zugriff auf alle Hosting-Zonen, die dem aktuellen AWS Konto gehören.
- Die zweite Anweisung erteilt Berechtigungen für alle Aktionen, die zum Erstellen und Verwalten von Zustandsprüfungen erforderlich sind.

Eine Liste der Aktionen mit den anzugebenden ARNs, mit denen ihnen Berechtigungen erteilt oder entzogen werden, finden Sie unter Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

Erforderliche Berechtigungen zur Verwendung der Amazon-Route-53-Konsole

Um Vollzugriff auf die Amazon-Route-53-Konsole zu gewähren, gewähren Sie die Berechtigungen in der folgenden Berechtigungsrichtlinie:

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:*",
                "route53domains:*",
                "tag:*",
                "ssm:GetParametersByPath",
```

```
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "sns:CreateTopic",
                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:Sign",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

Gründe, warum die Berechtigungen erforderlich sind

`route53:*`

Ermöglicht die Durchführung aller Route-53-Aktionen, mit Ausnahme der folgenden Aktionen:

- Erstellen und aktualisieren Sie Aliaseinträge, für die der Wert von Alias Target eine CloudFront Distribution, ein Elastic Load Balancing Load Balancer, eine Elastic Beanstalk Beanstalk-Umgebung oder ein Amazon S3 S3-Bucket ist. (Mit diesen Berechtigungen können Sie Alias-Datensätze erstellen, für die der Wert für Alias Target ein anderer Datensatz in der gleichen gehosteten Zone ist.)
- Arbeiten mit privaten gehosteten Zonen
- Arbeiten mit Domänen
- Alarme erstellen, löschen und anzeigen. CloudWatch
- Rendern Sie CloudWatch Metriken in der Route 53-Konsole.

`route53domains:*`

Ermöglicht Ihnen das Arbeiten mit Domänen.

> **Important**
>
> Wenn Sie `route53`-Aktionen einzeln auflisten, müssen Sie `route53:CreateHostedZone` für das Arbeiten mit Domänen angeben. Wenn Sie eine Domäne registrieren, wird gleichzeitig eine gehostete Zone erstellt. Also erfordert eine Richtlinie, die Berechtigungen zur Registrierung von Domänen enthält, auch eine Berechtigung zum Erstellen von gehosteten Zonen.

Bei der Domänenregistrierung wird die Erteilung oder Ablehnung von Berechtigungen für einzelne Ressourcen von Route 53 nicht unterstützt.

`route53resolver:*`

Ermöglicht die Arbeit mit Route 53 VPC Resolver.

`ssm:GetParametersByPath`

Ermöglicht das Abrufen öffentlich verfügbarer Regionen, wenn Sie neue Aliaseinträge, private gehostete Zonen und Zustandsprüfungen erstellen.

`cloudfront:ListDistributions`

Ermöglicht das Erstellen und Aktualisieren von Aliasdatensätzen, für die der Wert von Alias Target eine CloudFront Verteilung ist.

Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Verteilungen abzurufen und in der Konsole anzuzeigen.

`elasticloadbalancing:DescribeLoadBalancers`

Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Alias Target ein ELB-Load Balancer ist.

Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Load Balancer abzurufen und in der Konsole anzuzeigen.

`elasticbeanstalk:DescribeEnvironments`

Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel eine Elastic-Beanstalk-Umgebung ist.

Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Umgebungen abzurufen und in der Konsole anzuzeigen.

`s3:ListAllMyBuckets`, **`s3:GetBucketLocation`** und **`s3:GetBucketWebsite`**

Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel ein Amazon-S3-Bucket ist. (Sie können einen Alias für einen Amazon-S3-Bucket nur erstellen, wenn der Bucket als Website-Endpunkt konfiguriert ist; `s3:GetBucketWebsite` ruft die benötigten Konfigurationsinformationen ab.)

Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Buckets abzurufen und in der Konsole anzuzeigen.

`ec2:DescribeVpcs` und **`ec2:DescribeRegions`**

Ermöglicht das Arbeiten mit privaten gehosteten Zonen.

Alle aufgelisteten **`ec2`**-Berechtigungen

Lassen Sie Sie mit Route 53 VPC Resolver arbeiten.

`sns:ListTopics`, **`sns:ListSubscriptionsByTopic`**, **`sns:CreateTopic`**, **`cloudwatch:DescribeAlarms`**, **`cloudwatch:PutMetricAlarm`**, **`cloudwatch:DeleteAlarms`**

Ermöglicht das Erstellen, Löschen und Anzeigen CloudWatch von Alarmen.

`cloudwatch:GetMetricStatistics`

Ermöglicht die Erstellung von CloudWatch metrischen Zustandsprüfungen.

Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um Statistiken abzurufen und in der Konsole anzuzeigen.

`apigateway:GET`

Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel eine Amazon-API-Gateway-API ist.

Diese Berechtigung ist nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet es nur, um eine Liste von anzuzeigen APIs , die in der Konsole angezeigt werden sollen.

`kms:*`

Ermöglicht das Arbeiten mit, AWS KMS um die DNSSEC-Signatur zu aktivieren.

Beispielberechtigungen für einen Domänendatensatzbesitzer

Mithilfe von Berechtigungen für Ressourcendatensätze können Sie detaillierte Berechtigungen festlegen, die einschränken, was der AWS Benutzer aktualisieren oder ändern kann. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

In einigen Szenarien kann ein Besitzer einer gehosteten Zone für die Gesamtverwaltung der gehosteten Zone verantwortlich sein, während eine andere Person in der Organisation für eine Teilmenge dieser Aufgaben verantwortlich ist. Ein Besitzer einer gehosteten Zone, der die DNSSEC-Signatur aktiviert hat, möchte möglicherweise eine IAM-Richtlinie erstellen, die unter anderem die Erlaubnis für eine andere Person beinhaltet, Resource Set Records (RRs) in der gehosteten Zone hinzuzufügen und zu löschen. Die spezifischen Berechtigungen, die ein Besitzer einer gehosteten Zone für einen Datensatzbesitzer oder andere Personen aktiviert, hängen von der Richtlinie ihrer Organisation ab.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die es einem Datensatzbesitzer ermöglicht RRs, Änderungen an Verkehrsrichtlinien und Zustandsprüfungen vorzunehmen.
Ein Datensatzbesitzer mit dieser Richtlinie ist nicht berechtigt, Vorgänge auf Zonenebene durchzuführen, z. B. das Erstellen oder Löschen einer Zone, das Aktivieren oder Deaktivieren der

Abfrageprotokollierung, das Erstellen oder Löschen eines wiederverwendbaren Delegierungssatzes oder das Ändern von DNSSEC-Einstellungen.

```
{
      "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 vom Kunden verwaltete Schlüsselberechtigungen für DNSSEC-Signierung erforderlich

Wenn Sie die DNSSEC-Signatur für Route 53 aktivieren, erstellt Route 53 einen Schlüsselsignaturschlüssel (KSK), der auf einem vom Kunden verwalteten Schlüssel in () basiert. AWS Key Management Service AWS KMS Sie können einen vorhandenen vom Kunden verwalteten Schlüssel verwenden, der DNSSEC-Signatur unterstützt oder einen neuen Schlüssel erstellen. Route 53 muss über die Berechtigung verfügen, auf den vom Kunden verwalteten Schlüssel zuzugreifen, damit die KSK für Sie erstellt werden kann.

Um Route 53 für den Zugriff auf Ihren vom Kunden verwalteten Schlüssel zu aktivieren, stellen Sie sicher, dass die vom Kunden verwaltete Schlüsselrichtlinie die folgenden Anweisungen enthält:

```
{
            "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
                }
            }
        }
```

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, sie auszuführen. Um sich davor zu schützen, können Sie optional die Berechtigungen, die ein Dienst für eine Ressource hat, in einer ressourcenbasierten Richtlinie einschränken, indem Sie eine Kombination aus `aws:SourceAccount` und `aws:SourceArn` Bedingungen (beide oder eine) angeben. AWS KMS `aws:SourceAccount`ist eine AWS Konto-ID eines Besitzers einer gehosteten Zone. `aws:SourceArn`ist ein ARN einer gehosteten Zone.

Im Folgenden finden Sie zwei Beispiele für Berechtigungen, die Sie hinzufügen können:

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
```

```
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- Oder -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

Weitere Informationen finden Sie unter Das Problem des verwirrten Stellvertreters im IAM-Benutzerhandbuch.

Beispiele für vom Kunden verwaltete Richtlinien

Sie können eigene benutzerdefinierte IAM-Richtlinien erstellen, um Berechtigungen für Route-53-Aktionen zu erteilen. Sie können diese benutzerdefinierten Richtlinien den IAM-Gruppen anfügen, für die die angegebenen Berechtigungen erforderlich sind. Diese Richtlinien funktionieren, wenn Sie die Route 53-API AWS SDKs, die oder die AWS CLI verwenden. Die folgenden Beispiele zeigen Berechtigungen für einige häufige Anwendungsfälle. Weitere Informationen zu der Richtlinie, die Benutzern Vollzugriff auf Route 53 gewährt, finden Sie unter Erforderliche Berechtigungen zur Verwendung der Amazon-Route-53-Konsole.

Beispiele

- Beispiel 1: Lesezugriff auf alle gehosteten Zonen gewähren
- Beispiel 2: Erstellen und Löschen gehosteter Zonen zulassen
- Beispiel 3: Vollzugriff auf alle Domänen erlauben (nur öffentliche gehostete Zonen)

- Beispiel 4: Erstellung von eingehenden und ausgehenden Route 53 VPC Resolver-Endpunkten zulassen

Beispiel 1: Lesezugriff auf alle gehosteten Zonen gewähren

Die folgende Berechtigungsrichtlinie gewährt dem Benutzer Berechtigungen zum Auflisten aller gehosteten Zonen und zum Anzeigen aller Datensätze in einer gehosteten Zone.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

Beispiel 2: Erstellen und Löschen gehosteter Zonen zulassen

Die folgende Berechtigungsrichtlinie erlaubt es Benutzern, gehostete Zonen zu erstellen und zu löschen und den Fortschritt der Änderung zu verfolgen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
```

```
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

Beispiel 3: Vollzugriff auf alle Domänen erlauben (nur öffentliche gehostete Zonen)

Die folgende Berechtigungsrichtlinie erlaubt es Benutzern, alle Aktionen für die Domänenregistrierung durchzuführen (z. B. Berechtigungen zum Registrieren von Domänen und Erstellen gehosteter Zonen).

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Wenn Sie eine Domäne registrieren, wird gleichzeitig eine gehostete Zone erstellt. Also erfordert eine Richtlinie, die Berechtigungen zur Registrierung von Domänen enthält, auch Berechtigungen zum Erstellen von gehosteten Zonen. (Bei der Domänenregistrierung wird die Erteilung von Berechtigungen für einzelne Ressourcen von Route 53 nicht unterstützt.)

Weitere Informationen zu den Berechtigungen, die für das Arbeiten mit privaten gehosteten Zonen erforderlich sind, finden Sie unter Erforderliche Berechtigungen zur Verwendung der Amazon-Route-53-Konsole.

Beispiel 4: Erstellung von eingehenden und ausgehenden Route 53 VPC Resolver-Endpunkten zulassen

Mit der folgenden Berechtigungsrichtlinie können Benutzer die Route-53-Konsole verwenden, um eingehende und ausgehende Resolver-Endpunkte zu erstellen.

Einige dieser Berechtigungen sind nur zum Erstellen von Endpunkten in der Konsole erforderlich. Sie können diese Berechtigungen weglassen, wenn Sie Berechtigungen nur zum programmgesteuerten Erstellen eingehender und ausgehender Endpunkte erteilen möchten:

- Mit `route53resolver:ListResolverEndpoints` können Benutzer die Liste der eingehenden oder ausgehenden Endpunkte anzeigen, damit sie überprüfen können, ob ein Endpunkt erstellt wurde.
- `DescribeAvailabilityZones` ist erforderlich, um eine Liste der Availability Zones anzuzeigen.
- `DescribeVpcs`ist erforderlich, um eine Liste von anzuzeigen. VPCs

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "route53resolver:CreateResolverEndpoint",
                "route53resolver:ListResolverEndpoints",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon Route 53 Resolver

Route 53 VPC Resolver verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit VPC Resolver verknüpft ist. Dienstbezogene Rollen sind von VPC Resolver vordefiniert und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von VPC Resolver, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. VPC Resolver definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur VPC Resolver seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre VPC-Resolver-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-Linked Role (Serviceverknüpfte Rolle) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

- Dienstverknüpfte Rollenberechtigungen für VPC Resolver
- Eine serviceverknüpfte Rolle für VPC Resolver erstellen
- Bearbeiten einer serviceverknüpften Rolle für VPC Resolver
- Löschen einer serviceverknüpften Rolle für VPC Resolver
- Unterstützte Regionen für serviceverknüpfte VPC-Resolver-Rollen

Dienstverknüpfte Rollenberechtigungen für VPC Resolver

VPC Resolver verwendet die **`AWSServiceRoleForRoute53Resolver`**serviceverknüpfte Rolle, um Abfrageprotokolle in Ihrem Namen bereitzustellen.

Die Rollenberechtigungsrichtlinie ermöglicht es VPC Resolver, die folgenden Aktionen an Ihren Ressourcen durchzuführen:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für VPC Resolver erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Zuordnung zur Konfiguration des Resolver-Abfrageprotokolls in der Amazon Route 53 53-Konsole, der oder der AWS API erstellen AWS CLI, erstellt VPC Resolver die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Wenn Sie den VPC Resolver-Dienst vor dem 12. August 2020 verwendet haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat VPC Resolver die `AWSServiceRoleForRoute53Resolver` Rolle außerdem in Ihrem Konto erstellt. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine neue Konfigurationszuordnung für das Resolver-Abfrageprotokoll erstellen, wird die serviceverknüpfte `AWSServiceRoleForRoute53Resolver`-Rolle erneut für Sie erstellt.

Bearbeiten einer serviceverknüpften Rolle für VPC Resolver

Mit VPC Resolver können Sie die `AWSServiceRoleForRoute53Resolver` serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für VPC Resolver

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der VPC-Resolver-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um VPC-Resolver-Ressourcen zu löschen, die von **`AWSServiceRoleForRoute53Resolver`**

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter. https://console.aws.amazon.com/route53/
2. Erweitern Sie das Route-53-Konsolenmenü. Wählen Sie oben links in der Konsole die drei horizontalen Balken

   (☰)

   aus.
3. Wählen Sie im Resolver-Menü die Option Abfrageprotokollierung.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen Ihrer Abfrageprotokollierungskonfiguration, und wählen Sie dann Löschen aus.
5. Wählen Sie im Textfeld Konfiguration der Abfrageprotokollierung löschen die Option Protokollierungsabfragen beenden aus.

   Dadurch wird die Verbindung zwischen der Konfiguration und der VPC getrennt. Sie können die Zuordnung der Konfiguration der Abfrageprotokollierung auch programmgesteuert aufheben. Weitere Informationen finden Sie unter disassociate-resolver-query-log-config.
6. Nachdem die Protokollierung von Abfragen beendet wurde, können Sie optional **`delete`** in das Feld eingeben und Löschen wählen, um die Abfrageprotokollierungskonfiguration zu löschen. Dies ist jedoch nicht erforderlich, um die von `AWSServiceRoleForRoute53Resolver`verwendeten Ressourcen zu löschen.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForRoute53Resolver` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte VPC-Resolver-Rollen

VPC Resolver unterstützt nicht die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Sie können die Rolle `AWSServiceRoleForRoute53Resolver` in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support in VPC Resolver
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Paris)	eu-west-3	Ja
Südamerika (São Paulo)	sa-east-1	Ja
China (Peking)	cn-north-1	Ja
China (Ningxia)	cn-northwest-1	Ja
AWS GovCloud (US)	us-gov-east-1	Ja
AWS GovCloud (US)	us-gov-west-1	Ja

AWS verwaltete Richtlinien für Amazon Route 53

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AmazonRoute 53 FullAccess

Sie können die `AmazonRoute53FullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt vollen Zugriff auf Route 53-Ressourcen, einschließlich Domainregistrierung und Integritätsprüfung, jedoch ohne VPC Resolver.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53:*` – Ermöglicht die Durchführung aller Route-53-Aktionen, mit Ausnahme der folgenden Aktionen:
  - Erstellen und aktualisieren Sie Aliaseinträge, für die der Wert von Alias Target eine CloudFront Distribution, ein Elastic Load Balancing Load Balancer, eine Elastic Beanstalk Beanstalk-Umgebung oder ein Amazon S3 S3-Bucket ist. (Mit diesen Berechtigungen können Sie Alias-Datensätze erstellen, für die der Wert für Alias Target ein anderer Datensatz in der gleichen gehosteten Zone ist.)
  - Arbeiten mit privaten gehosteten Zonen
  - Arbeiten mit Domänen

  - Alarme erstellen, löschen und anzeigen. CloudWatch
  - Rendern Sie CloudWatch Metriken in der Route 53-Konsole.
- `route53domains:*` – Ermöglicht Ihnen das Arbeiten mit Domänen.
- `cloudfront:ListDistributions`— Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert von Alias Target eine CloudFront Verteilung ist.

  Diese Berechtigung ist nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Verteilungen abzurufen und in der Konsole anzuzeigen.
- `cloudfront:GetDistributionTenantByDomain`— Wird verwendet, um die CloudFront Mehrmandantenverteilungen abzurufen, sodass Sie Aliasdatensätze erstellen und aktualisieren können, für die der Wert von Alias Target ein CloudFront Verteilungsmandant ist.
- `cloudfront:GetConnectionGroup`— Wird verwendet, um die CloudFront Mehrmandantenverteilungen abzurufen, sodass Sie Aliasdatensätze erstellen und aktualisieren können, für die der Wert von Alias Target ein Verteilungsmandant ist. CloudFront
- `cloudwatch:DescribeAlarms`— Ermöglicht zusammen mit `sns:ListTopics` und `sns:ListSubscriptionsByTopic` das Erstellen, Löschen und Anzeigen von Alarmen. CloudWatch
- `cloudwatch:GetMetricStatistics`— Ermöglicht die Erstellung von CloudWatch metrischen Zustandsprüfungen.

  Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um Statistiken abzurufen und in der Konsole anzuzeigen.
- `cloudwatch:GetMetricData`— Ermöglicht es Ihnen, den Status Ihrer CloudWatch Gesundheitscheck-Metriken anzuzeigen.
- `ec2:DescribeVpcs`— Ermöglicht das Anzeigen einer Liste von VPCs.
- `ec2:DescribeVpcEndpoints` – Ermöglicht das Anzeigen einer Liste von VPC Endpunkten.
- `ec2:DescribeRegions` – Ermöglicht Ihnen das Anzeigen einer Liste von Availability Zones.
- `elasticloadbalancing:DescribeLoadBalancers` – Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel ein Elastic-Load-Balancing-Load-Balancer ist.

  Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Load Balancer abzurufen und in der Konsole anzuzeigen.

- `elasticbeanstalk:DescribeEnvironments` – Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel eine Elastic-Beanstalk-Umgebung ist.

  Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Umgebungen abzurufen und in der Konsole anzuzeigen.
- `es:ListDomainNames`— Ermöglicht die Anzeige der Namen aller Amazon OpenSearch Service-Domains, die dem aktuellen Benutzer in der aktiven Region gehören.
- `es:DescribeDomains`— Ermöglicht das Abrufen der Domain-Konfiguration für die angegebenen Amazon OpenSearch Service-Domains.
- `lightsail:GetContainerServices`— Ermöglicht Ihnen die Lightsail-Container-Dienste, mit denen Sie Alias-Datensätze erstellen und aktualisieren können, für die der Wert von Alias Target eine Lightsail-Domain ist.
- `s3:ListBucket`, `s3:GetBucketLocation`, und `s3:GetBucketWebsite` – Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel ein Amazon-S3-Bucket ist. (Sie können einen Alias für einen Amazon-S3-Bucket nur erstellen, wenn der Bucket als Website-Endpunkt konfiguriert ist; `s3:GetBucketWebsite` ruft die benötigten Konfigurationsinformationen ab.)

  Diese Berechtigungen sind nicht erforderlich, wenn Sie die Route-53-Konsole nicht verwenden. Route 53 verwendet sie nur, um eine Liste der Buckets abzurufen und in der Konsole anzuzeigen.
- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Ermöglicht das Erstellen, Löschen und Anzeigen von Alarmen. CloudWatch
- `tag:GetResources`— Ermöglicht die Anzeige der Tags in Ihren Ressourcen. Zum Beispiel die Namen Ihrer Gesundheitschecks.
- `apigateway:GET` – Ermöglicht das Erstellen und Aktualisieren von Alias-Datensätzen, für die der Wert für Aliasziel eine Amazon-API-Gateway-API ist.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
```

```
  {
   "Effect": "Allow",
   "Action": [
    "route53:*",
    "route53domains:*",
    "cloudfront:ListDistributions",
    "cloudfront:GetDistributionTenantByDomain",
    "cloudfront:GetConnectionGroup",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:GetMetricData",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeRegions",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticbeanstalk:DescribeEnvironments",
    "es:ListDomainNames",
    "es:DescribeDomains",
    "lightsail:GetContainerServices",
    "s3:ListBucket",
    "s3:GetBucketLocation",
    "s3:GetBucketWebsite",
    "sns:ListTopics",
    "sns:ListSubscriptionsByTopic",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "apigateway:GET",
   "Resource": "arn:aws:apigateway:*::/domainnames"
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ReadOnlyAccess

Sie können die `AmazonRoute53ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt schreibgeschützten Zugriff auf Route 53-Ressourcen, einschließlich Domänenregistrierung und Integritätsprüfung, jedoch ohne VPC Resolver.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53:Get*` – Ruft die Route-53-Ressourcen ab.
- `route53:List*` – Listet die Route-53-Ressourcen auf.
- `route53:TestDNSAnswer` – Ruft den Wert ab, den Route 53 als Antwort auf eine DNS-Anforderung zurückgibt.

Weitere Informationen zu den Berechtigungen finden Sie unter. Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 DomainsFullAccess

Sie können die `AmazonRoute53DomainsFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt uneingeschränkten Zugriff auf Route-53-Domänenregistrierungsressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53:CreateHostedZone` – Ermöglicht Ihnen das Erstellen einer von Route 53 gehosteten Zone.
- `route53domains:*` – Ermöglicht das Registrieren von Domänennamen und das Ausführen zugehöriger Vorgänge.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 DomainsReadOnlyAccess

Sie können die `AmazonRoute53DomainsReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Nur-Lesen-Zugriff auf Route-53-Domänenregistrierungsressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53domains:Get*` – Ermöglicht das Abrufen einer Liste von Domänen von Route 53.
- `route53domains:List*` – Hier können Sie eine Liste der Route-53-Domänen anzeigen.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ResolverFullAccess

Sie können die `AmazonRoute53ResolverFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt vollen Zugriff auf Route 53 VPC Resolver-Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53resolver:*`— Ermöglicht das Erstellen und Verwalten von VPC-Resolver-Ressourcen auf der Route 53-Konsole.
- `ec2:DescribeSubnets` – Ermöglicht das Auflisten Ihrer Amazon-VPC-Subnetze.
- `ec2:CreateNetworkInterface`, `ec2:DeleteNetworkInterface` und `ec2:ModifyNetworkInterfaceAttribute` – Ermöglicht das Erstellen, Ändern und Löschen von Netzwerkschnittstellen.
- `ec2:DescribeNetworkInterfaces` – Hiermit können Sie eine Liste der Netzwerkschnittstellen anzeigen.

- `ec2:DescribeSecurityGroups` – Ermöglicht Ihnen das Anzeigen einer Liste mit all Ihren Sicherheitsgruppen.
- `ec2:DescribeVpcs`— Ermöglicht das Anzeigen einer Liste von. VPCs
- `ec2:DescribeAvailabilityZones` – Ermöglicht Ihnen das Auflisten der Zonen, die für Sie verfügbar sind.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ResolverReadOnlyAccess

Sie können die `AmazonRoute53ResolverReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt schreibgeschützten Zugriff auf Route 53 VPC Resolver-Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53resolver:Get*`— Ruft VPC-Resolver-Ressourcen ab.
- `route53resolver:List*`— Ermöglicht das Anzeigen einer Liste von VPC-Resolver-Ressourcen.
- `ec2:DescribeNetworkInterfaces` – Hiermit können Sie eine Liste der Netzwerkschnittstellen anzeigen.
- `ec2:DescribeSecurityGroups` – Ermöglicht Ihnen das Anzeigen einer Liste mit all Ihren Sicherheitsgruppen.

Weitere Informationen zu den Berechtigungen finden Sie unter. Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: Route53 ResolverServiceRolePolicy

Sie können `Route53ResolverServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es Route 53 VPC Resolver ermöglicht, auf AWS Dienste und Ressourcen zuzugreifen, die von VPC Resolver verwendet oder verwaltet werden. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Route 53 Resolver.

AWS verwaltete Richtlinie: 53 AmazonRoute ProfilesFullAccess

Sie können die `AmazonRoute53ProfilesReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt vollen Zugriff auf die Amazon Route 53 53-Profilressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53profiles`— Ermöglicht das Erstellen und Verwalten von Profilressourcen auf der Route 53-Konsole.
- `ec2`— Ermöglicht Prinzipalen das Abrufen von Informationen über VPCs.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:PutProfilePolicy",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ProfilesReadOnlyAccess

Sie können die `AmazonRoute53ProfilesReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt nur Lesezugriff auf Amazon Route 53 53-Profilressourcen.

Details zu Berechtigungen

Weitere Informationen zu den Berechtigungen finden Sie unter. Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Leiten Sie 53-Updates an AWS verwaltete Richtlinien weiter

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Route 53 an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite erhalten, abonnieren Sie den RSS-Feed auf der Route-53-Dokumentverlauf-Seite.

Änderungen	Beschreibung	Date
AmazonRoute53 FullAccess — Aktualisierte Richtlinie	Fügt Berechtigungen für `cloudwatch:GetMetricData tag:GetResources ,es:ListDomainNames , es:DescribeDomains cloudfront:GetDistributionTenantByDomain , cloudfront:GetConnectionGroup` und hinzu`lightsail:GetContainerServices` . Mit diesen Berechtigungen können Sie bis zu 500 CloudWatch Health Check-Metriken und bis zu 100 Namen von Zustandsprüfungen abrufen, die Domain-Konfiguration für die angegebenen Amazon OpenSearch Service-Domains abrufen und die Namen aller Amazon OpenSearch Service-Domains auflisten, die dem aktuellen Benutzer in der aktiven Region gehören, die CloudFront Multi-Tenant-Distributionen abrufen und die Lightsail-Container-Services abrufen.	01. Juni 2025
AmazonRoute53 ProfilesFullAccess — Aktualisierte Richtlinie	Fügt Berechtigungen für `GetProfilePolicy` und hinzu`PutProfilePolicy` .	27. August 2024

Änderungen	Beschreibung	Date
	Dies sind IAM-Aktionen, die nur für Berechtigungen gelten. Wenn einem IAM-Prinzipal diese Berechtigungen nicht erteilt wurden, tritt beim Versuch, das Profil mithilfe des AWS RAM Dienstes freizugeben, ein Fehler auf.	
AmazonRoute53 ProfilesReadOnlyAccess — Aktualisierte Richtlinie	Fügt Berechtigungen hinzu für`GetProfilePolicy` . Dies ist eine IAM-Aktion, für die nur Berechtigungen erforderlich sind. Wenn einem IAM-Prinzipal diese Berechtigung nicht erteilt wurde, tritt beim Versuch, mithilfe des Dienstes auf die Richtlinie des Profils zuzugreifen, ein Fehler auf. AWS RAM	27. August 2024
AmazonRoute53 ResolverFullAccess — Aktualisierte Richtlinie	Es wurde eine Kontoausweis-ID (Sid) hinzugefügt, um die Richtlinie eindeutig zu identifizieren.	5. August 2024
AmazonRoute53 ResolverReadOnlyAccess — Aktualisierte Richtlinie	Es wurde eine Kontoausweis-ID (Sid) hinzugefügt, um die Richtlinie eindeutig zu identifizieren.	5. August 2024
AmazonRoute53 — Neue Richtlinie ProfilesFullAccess	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf Amazon Route 53 53-Profilressourcen zu ermöglichen.	22. April 2024

Änderungen	Beschreibung	Date
AmazonRoute53 ProfilesReadOnlyAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, die den schreibgeschützten Zugriff auf Amazon Route 53 53-Profilressourcen ermöglicht.	22. April 2024
Route53 ResolverServiceRolePolicy — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, die an eine serviceverknüpfte Rolle angehängt ist und es VPC Resolver ermöglicht, auf AWS Services und Ressourcen zuzugreifen, die von Resolver verwendet oder verwaltet werden.	14. Juli 2021
AmazonRoute53 — Neue Richtlinie ResolverReadOnlyAccess	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, die den schreibgeschützten Zugriff auf VPC-Resolver-Ressourcen ermöglicht.	14. Juli 2021
AmazonRoute53 — Neue Richtlinie ResolverFullAccess	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf VPC-Resolver-Ressourcen zu ermöglichen.	14. Juli 2021
AmazonRoute53 DomainsReadOnlyAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um den schreibgeschützten Zugriff auf Route 53-Domänenressourcen zu ermöglichen.	14. Juli 2021

Änderungen	Beschreibung	Date
AmazonRoute53 DomainsFullAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf Route 53-Domänenressourcen zu ermöglichen.	14. Juli 2021
AmazonRoute53 ReadOnlyAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um den schreibgeschützten Zugriff auf Route 53-Ressourcen zu ermöglichen.	14. Juli 2021
AmazonRoute53 FullAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf Route 53-Ressourcen zu ermöglichen.	14. Juli 2021
Route 53 hat begonnen, Änderungen zu verfolgen	Route 53 hat damit begonnen, Änderungen für seine AWS verwalteten Richtlinien nachzuverfolgen.	14. Juli 2021

Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle

In Route 53 können Sie Bedingungen angeben, wenn Sie Berechtigungen mithilfe einer IAM-Richtlinie erteilen (siehe Zugriffskontrolle). Beispielsweise ist Folgendes möglich:

- Erteilen Sie Berechtigungen, um Zugriff auf einen einzelnen Ressourcendatensatz zu gewähren.
- Gewähren Sie Berechtigungen, um Benutzern Zugriff auf alle Ressourceneintragssätze eines bestimmten DNS-Eintragstyps in einer gehosteten Zone zu gewähren, z. B. A- und AAAA-Datensätze.

- Gewähren Sie Berechtigungen, um Benutzern den Zugriff auf einen Ressourcendatensatz zu ermöglichen, dessen Name eine bestimmte Zeichenfolge enthält.
- Gewähren Sie Benutzern Berechtigungen, damit sie nur einen Teil der `CREATE | UPSERT | DELETE` Aktionen auf der Route 53-Konsole oder bei Verwendung der API ausführen können. ChangeResourceRecordSets
- Gewähren Sie Benutzern Berechtigungen, die es Benutzern ermöglichen, private gehostete Zonen einer bestimmten VPC zuzuordnen oder von ihr zu trennen.
- Erteilen Sie Berechtigungen, damit Benutzer gehostete Zonen auflisten können, die einer bestimmten VPC zugeordnet sind.
- Erteilen Sie Berechtigungen, um Benutzern Zugriff auf die Erstellung einer neuen privaten gehosteten Zone und deren Zuordnung zu einer bestimmten VPC zu gewähren.
- Erteilen Sie Berechtigungen, damit Benutzer eine VPC-Zuordnungsautorisierung erstellen oder löschen können.

Sie können auch Berechtigungen erstellen, die eine der detaillierten Berechtigungen kombinieren.

Normalisierung der Schlüsselwerte der Route 53-Bedingung

Die Werte, die Sie für die Richtlinienbedingungen eingeben, müssen wie folgt formatiert oder normalisiert sein:

Für **`route53:ChangeResourceRecordSetsNormalizedRecordNames`**:

- Alle Buchstaben müssen Kleinbuchstaben sein.
- Der DNS-Name muss ohne den letzten Punkt sein.
- Andere Zeichen als a–z, 0–9, - (Bindestrich), _ (Unterstrich) und . (Punkt, als Trennzeichen zwischen Kennzeichnungen) müssen Escape-Codes im Format \dreistelliger Oktalcode verwenden. Zum Beispiel ist `\052` der Oktalcode für das Zeichen *.

Für **`route53:ChangeResourceRecordSetsActions`** kann der Wert einer der folgenden Möglichkeiten sein und muss in Großbuchstaben sein:

- CREATE
- UPSERT
- DELETE

Für **`route53:ChangeResourceRecordSetsRecordTypes`**:

- Der Wert muss in Großbuchstaben geschrieben werden und kann einer der von Route 53 unterstützten DNS-Eintragstypen sein. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Für **`route53:VPCs`**:

- Der Wert muss das Format von `VPCId=<vpc-id>,VPCRegion=<region>` haben.
- Der Wert von `<vpc-id>` und `<region>` muss in Kleinbuchstaben angegeben werden, z. B. `VPCId=vpc-123abc` und`VPCRegion=us-east-1`.
- Bei den Kontextschlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden.

> **Important**
>
> Damit Ihre Berechtigungen Aktionen wie gewünscht zulassen oder einschränken können, müssen Sie diese Konventionen befolgen. Nur `VPCId` `VPCRegion` Elemente werden von diesem Bedingungsschlüssel akzeptiert, andere AWS Ressourcen, wie z. B. AWS-Konto, werden nicht unterstützt.

Sie können den Access Analyzer oder Richtliniensimulator im IAM-Benutzerhandbuch nutzen, um zu überprüfen, ob Ihre Richtlinie die Berechtigungen wie erwartet gewährt oder einschränkt. Sie können die Berechtigungen auch überprüfen, indem Sie eine IAM-Richtlinie auf einen Testbenutzer oder eine Testrolle anwenden, um Route 53-Vorgänge auszuführen.

Festlegung von Bedingungen: Verwenden von Bedingungsschlüsseln

AWS stellt einen Satz vordefinierter Bedingungsschlüssel (für alle AWS Bedingungsschlüssel) für alle AWS Dienste bereit, die IAM für die Zugriffskontrolle unterstützen. Sie können beispielsweise den `aws:SourceIp`-Bedingungsschlüssel verwenden, um die IP-Adresse des Anforderers zu prüfen, bevor eine Aktion durchgeführt werden darf. Weiter Informationen und eine Liste von AWS-weiten Schlüsseln finden Sie unter Verfügbare Schlüssel für Bedingungen im IAM-Benutzerhandbuch.

> **Note**
>
> Route 53 unterstützt keine tag-basierten Bedingungsschlüssel.

In der folgenden Tabelle sind die dienstspezifischen Bedingungsschlüssel für Route 53 aufgeführt, die für Route 53 gelten.

Route 53-Bedingungsschlüssel	API-Operationen	Werttyp	Description
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	Mehrwertig	Stellt eine Liste von DNS-Eintragsnamen in der Anfrage von ChangeResourceRecordSets dar. Um das erwartete Verhalten zu erhalten, müssen DNS-Namen in der IAM-Richtlinie wie folgt normalisiert werden: • Alle Buchstaben müssen Kleinbuchstaben sein. • Der DNS-Name muss ohne den letzten Punkt sein. • Andere Zeichen als a–z, 0 bis 9, - (Bindestrich), _ (Unterstrich) und . (Punkt, als Trennzeichen zwischen Kennzeichnungen) muss Escape-Codes im Format \dreistelliger Oktalcode verwenden.
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	Mehrwertig	Stellt eine Liste von DNS-Eintragstypen in der Anforderung von `ChangeResourceRecordSets` dar. `ChangeResourceRecordSetsRecordTypes` kann jeder der von Route 53 unterstützten DNS-Eintragstypen sein. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen. Alle müssen in der Richtlinie in Großbuchstaben eingegeben werden.

Route 53-Bedingungsschlüssel	API-Operationen	Werttyp	Description
`route53:ChangeResourceRecordSetsActions`	ChangeResourceRecordSets	Mehrwertig	Stellt eine Liste von Aktionen in der Anforderung von `ChangeResourceRecordSets` dar. `ChangeResourceRecordSetsActions` kann jeder der folgenden Werte sein (muss in Großbuchstaben sein): • CREATE • UPSERT • DELETE

Route 53-Bedingungsschlüssel	API-Operationen	Werttyp	Description
`route53:VPCs`	AssoziierenVPCWithHostedZone TrennenVPCFromHostedZone ListHostedZonesByVPC CreateHostedZone AutorisierungerstellenVPCAssociation VPCAssociationAutorisierunglöschen	Mehrwertig	Stellt eine Liste von VPCs in der Anfrage von`AssociateVPCWithHostedZone` ,`DisassociateVPCFromHostedZone` , `ListHostedZonesByVPC` `CreateHostedZone` ,`CreateVPCAssociationAuthorization` , und`DeleteVPCAssociationAuthorization` , und, im Format "VPCId=<vpc-id>, VPCRegion = <region>

Beispielrichtlinien: Verwenden von Bedingungen für differenzierten Zugriff

Jedes der Beispiele im folgenden Abschnitt legt die Effektklausel auf „erlauben“ fest und gibt nur die Aktionen, Ressourcen und Parameter an, die erlaubt sind. Zugriff hat lediglich das, was in der IAM-Richtlinie aufgeführt ist.

In einigen Fällen ist es möglich, diese Richtlinien umzuschreiben, damit sie auf Verweigerung basieren (dies bedeutet, die Effektklausel auf „verweigern“ festzulegen und die gesamte Logik in

der Richtlinie umzukehren). Allerdings empfehlen wir, dass Sie die Nutzung von Richtlinien, die auf Verweigerung basieren vermeiden, weil es verglichen mit Richtlinien, die auf Berechtigung basieren, schwierig ist, sie korrekt zu schreiben. Dies gilt insbesondere für Route 53 aufgrund der erforderlichen Textnormalisierung.

Berechtigungen erteilen, die den Zugriff auf DNS-Einträge mit bestimmten Namen beschränken

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen, die `ChangeResourceRecordSets`-Aktionen in der gehosteten Zone Z12345 für example.com and marketing.example.com erlauben. Sie benutzt den `route53:ChangeResourceRecordSetsNormalizedRecordNames`-Bedingungsschlüssel, um Benutzeraktionen nur auf die Datensätze zu beschränken, die den angegebenen Namen entsprechen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z111111122222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com", "marketing.example.com"]
                }
            }
          }
        ]
}
```

`ForAllValues:StringEquals` ist ein IAM-Bedingungsoperator, der für mehrwertige Schlüssel gilt. Die Bedingung in der obigen Richtlinie erlaubt den Vorgang nur, wenn alle Änderungen in `ChangeResourceRecordSets` den DNS-Namen example.com haben. Weitere Informationen finden Sie unter IAM-Bedingungsoperatoren undIAM-Bedingung mit mehreren Schlüsseln oder Werten im IAM-Benutzerhandbuch.

Um die Berechtigung zu implementieren, die Namen mit bestimmten Suffixen abgleicht, können Sie den IAM-Platzhalter (*) in der Richtlinie mit Bedingungsoperator `StringLike` oder `StringNotLike` verwenden. Die folgende Richtlinie erlaubt den Vorgang, wenn alle Änderungen in der Operation `ChangeResourceRecordSets` DNS-Namen haben, die mit „-beta.example.com“ enden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringLike":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["*-beta.example.com"]
                }
            }
          }
        ]
}
```

> **Note**
>
> Der IAM-Platzhalter ist nicht derselbe wie der Platzhalter für den Domänennamen. Im folgenden Beispiel wird gezeigt, wie der Platzhalter mit einem Domänennamen verwendet wird.

Gewähren Sie Berechtigungen, die den Zugriff auf DNS-Einträge einschränken, die mit einem Domänennamen mit Platzhalter übereinstimmen

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen, die `ChangeResourceRecordSets`-Aktionen in der gehosteten Zone Z12345 für example.com erlauben. Er benutzt den Bedingungsschlüssel `route53:ChangeResourceRecordSetsNormalizedRecordNames`, um Benutzeraktionen nur auf die Datensätze zu beschränken, die mit *.example.com übereinstimmen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["\
\052.example.com"]
                }
            }
          }
        ]
}
```

`\052` ist der Oktalcode für das Zeichen * im DNS-Namen und \ in `\052` ist entkommen, um `\\` zu sein, um JSON-Syntax zu folgen.

Berechtigungen erteilen, die den Zugriff auf bestimmte DNS-Einträge beschränken

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen, die `ChangeResourceRecordSets`-Aktionen in der gehosteten Zone Z12345 für example.com erlauben. Verwendet die Kombination von drei Bedingungsschlüsseln, um Benutzeraktionen so zu beschränken, dass nur DNS-Einträge mit einem bestimmten DNS-Namen und -Typ erstellt oder bearbeitet werden können.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
```

```
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com"],
                    "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],
                    "route53:ChangeResourceRecordSetsActions": ["CREATE",
 "UPSERT"]
                }
            }
          }
        ]
}
```

Berechtigungen erteilen, die den Zugriff auf die Erstellung und Bearbeitung nur der angegebenen Typen von DNS-Einträgen beschränken

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen, die `ChangeResourceRecordSets`-Aktionen in der gehosteten Zone Z12345 für example.com erlauben. Sie benutzt den Bedingungsschlüssel `route53:ChangeResourceRecordSetsRecordTypes`, um Benutzeraktionen nur auf die Datensätze zu beschränken, die den angegebenen Typen (A und AAAA) entsprechen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

Gewähren Sie Berechtigungen, die die VPC angeben, in der der IAM-Prinzipal arbeiten kann

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen,`AssociateVPCWithHostedZone`,`DisassociateVPCFromHostedZone`, `ListHostedZonesByVPC` `CreateHostedZoneCreateVPCAssociationAuthorization`, und `DeleteVPCAssociationAuthorization` Aktionen auf der durch die VPC-ID angegebenen VPC.

> **Important**
>
> Der Bedingungswert muss das Format von haben. `VPCId=<vpc-id>,VPCRegion=<region>` Wenn Sie im Bedingungswert einen VPC-ARN angeben, wird der Bedingungsschlüssel nicht wirksam.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "route53:*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "route53:VPCs": [
                        "VPCId=<vpc-id>,VPCRegion=<region>"
                    ]
                }
            }
        },
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcs",
            "Resource": "*"
        }
    ]
```

```
}
```

Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

Wenn Sie eine Berechtigungsrichtlinie einrichten Zugriffskontrolle und schreiben, die Sie einer IAM-Identität zuordnen können (identitätsbasierte Richtlinien), können Sie die Listen der Aktionen, Ressourcen und Bedingungsschlüssel für Route 53, Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domänen, Aktionen, Ressourcen und Bedingungsschlüssel für VPC Resolver und Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53 Profiles verwenden, um DNS-Einstellungen mit VPCs in der Service Authorization Reference zu teilen. Die Seiten enthalten jede Amazon Route 53-API-Aktion, die Aktionen, für die Sie Zugriffsberechtigungen gewähren müssen, und die AWS Ressource, für die Sie Zugriff gewähren müssen. Die Aktionen geben Sie im Feld `Action` und den Wert für die Ressource im Feld `Resource` der Richtlinie an.

Sie können in Ihren Route 53-Richtlinien allgemeine Bedingungsschlüssel verwenden AWS, um Bedingungen auszudrücken. Eine vollständige Liste der AWS-weiten Schlüssel finden Sie unter Verfügbare Schlüssel im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn Zugriff gewährt wird, müssen die gehostete Zone und die Amazon VPC zur selben Partition gehören. Eine Partition ist eine Gruppe von. AWS-Regionen Jede AWS-Konto ist auf eine Partition beschränkt.
> Im Folgenden werden die unterstützten Partitionen angezeigt:
>
> - `aws` - AWS-Regionen
> - `aws-cn` – Chinesiche Regionen
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> Weitere Informationen finden Sie unter Access Management (Zugriffsverwaltung) in der allgemeinen Referenz zu AWS .

> **Note**
>
> Um eine Aktion anzugeben, verwenden Sie das gültige Präfix (`route53`, `route53domains` oder `route53resolver`) gefolgt vom Namen der API-Operation, z. B.:
>
> - `route53:CreateHostedZone`
> - `route53domains:RegisterDomain`
> - `route53resolver:CreateResolverEndpoint`

Protokollierung und Überwachung in Amazon Route 53

Amazon Route 53 bietet die Protokollierung von DNS-Abfragen und die Möglichkeit, Ihre Ressourcen mithilfe von Zustandsprüfungen überwachen. Darüber hinaus lässt sich Route 53 in andere AWS Dienste integrieren, um zusätzliche Protokollierung und Überwachung zu ermöglichen:

Protokollierung von DNS-Abfragen

Sie können Route 53 so konfigurieren, dass Informationen zu den Abfragen protokolliert werden, die Route 53 erhält, wie z. B. die Domain oder Subdomain, die angefordert wurde, das Datum und die Uhrzeit der Anforderung und die DNS-Datensatztyp (z. B. A oder AAAA).

Weitere Informationen finden Sie unter Öffentliche DNS-Abfrageprotokollierung.

Wird AWS CloudTrail zur Protokollierung von Konsolen- und programmatischen Aktionen verwendet

CloudTrail bietet eine Aufzeichnung der Route 53-Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführt wurden. Anhand der von CloudTrail gesammelten Informationen können Sie nachverfolgen, welche Anfragen gestellt wurden, von welchen IP-Adressen Anfragen stammen, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Details. Weitere Informationen finden Sie unter Protokollieren von Amazon Route 53-API-Aufrufen mit AWS CloudTrail.

Überwachung von Domainregistrierungen

Das Route-53-Dashboard liefert detaillierte Informationen über den Status Ihrer Domainregistrierungen, wie z. B. den Status von Domainübertragungen und Domains, die kurz vor dem Ablaufdatum stehen.

Weitere Informationen finden Sie unter Überwachung von Domainregistrierungen.

Verwenden Sie Route 53-Zustandsprüfungen und Amazon CloudWatch zur Überwachung Ihrer Ressourcen

Sie können Ihre Ressourcen überwachen, indem Sie Route 53-Zustandsprüfungen erstellen, bei denen Rohdaten gesammelt und CloudWatch zu lesbaren Metriken verarbeitet werden, die nahezu in Echtzeit verfügbar sind.

Weitere Informationen finden Sie unter Überwachen Sie Ihre Ressourcen mit Amazon Route 53 Health Checks und Amazon CloudWatch.

Verwendung von Amazon CloudWatch zur Überwachung von Route 53 VPC Resolver-Endpunkten

Sie können CloudWatch damit die Anzahl der DNS-Abfragen überwachen, die von Resolver-Endpunkten weitergeleitet werden.

Weitere Informationen finden Sie unter Überwachung von Route 53 VPC Resolver-Endpunkten mit Amazon CloudWatch.

Verwenden AWS Trusted Advisor

Trusted Advisor stützt sich auf bewährte Verfahren, die bei der AWS Kundenbetreuung gelernt wurden. Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, wenn es Möglichkeiten gibt, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Alle AWS Kunden haben Zugriff auf fünf Trusted Advisor Schecks. Kunden mit einem Business- oder Enterprise-Supportplan können alle Trusted Advisor Schecks einsehen.

Weitere Informationen finden Sie unter Trusted Advisor.

Compliance-Validierung für Amazon Route 53

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon Route 53 im Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS Services im Umfang nach Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS -Compliance-Programme.

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte in AWS Artifact herunterladen.

Ihre Compliance-Verantwortung bei Verwendung von Route 53 hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. Wenn Ihre Nutzung von Route 53 der Einhaltung von Standards wie HIPAA, PCI oder FedRAMP unterliegt, AWS bietet Ihnen folgende Ressourcen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Config— Mit diesem AWS Service wird bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche zu überprüfen.

Ausfallsicherheit in Amazon Route 53

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Route 53 unterteilt seine Funktionalität in eine Steuer- und Datenebene. Route 53 Service enthält – wie die meisten AWS -Services – eine Steuerebene, mit der Sie Verwaltungsvorgänge wie das Erstellen, Aktualisieren und Löschen von Ressourcen ausführen können, sowie eine Datenebene, die die Kernfunktionalität des Dienstes bereitstellt. Weitere Informationen zu Steuer- und Datenebenen in Route 53 finden Sie unter Konzepte für Steuer- und Datenebene.

Route 53 ist in erster Linie ein globaler Dienst, aber die folgenden Funktionen unterstützen AWS Regionen:

- Wenn Sie Route 53 VPC Resolver zum Einrichten von Hybridkonfigurationen verwenden, erstellen Sie Endpoints in von Ihnen ausgewählten AWS Regionen und geben IP-Adressen in mehreren Availability Zones an. Für ausgehende Endpunkte können Sie Regeln in der gleichen Region, in der Sie den Endpunkt erstellt haben, erstellen. Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.
- Sie können Route 53-Zustandsprüfungen konfigurieren, um den Zustand von Ressourcen zu überprüfen, die Sie in bestimmten Regionen erstellen, z. B. EC2 Amazon-Instances und Elastic Load Balancing Load Balancer.
- Wenn Sie eine Zustandsprüfung erstellen, die einen Endpunkt überwacht, können Sie optional die Regionen angeben, von denen Route 53 Zustandsprüfungen durchführen soll.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in Amazon Route 53

Als verwalteter Service ist Amazon Route 53 durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Route 53 zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Ergebnisse von der Resolver DNS Firewall an Security Hub CSPM senden

AWS Security Hub CSPMbietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub CSPM sammelt Sicherheitsdaten von allen AWS-Konten und unterstützten Produkten von Drittanbietern und hilft Ihnen dabei, Sicherheitstrends zu analysieren und Sicherheitsprobleme mit der höchsten Priorität zu identifizieren. AWS-Services

Durch die Integration der Resolver DNS Firewall in Security Hub CSPM können Sie Ergebnisse von der DNS-Firewall an Security Hub CSPM senden. Security Hub CSPM bezieht diese Ergebnisse dann in die Analyse Ihres Sicherheitsstatus ein.

Inhalt

So funktionieren die Ergebnisse in Security Hub CSPM

In Security Hub CSPM ist ein Befund eine beobachtbare Aufzeichnung einer Sicherheitsüberprüfung oder einer sicherheitsrelevanten Entdeckung. Einige Ergebnisse beruhen auf Problemen, die von anderen oder AWS-Services von Drittanbietern entdeckt wurden. Security Hub CSPM verfügt auch über eigene Sicherheitskontrollen, mit denen Sicherheitsprobleme erkannt und Ergebnisse generiert werden.

Security Hub CSPM bietet Tools zur Verwaltung von Ergebnissen aus all diesen Quellen. Sie können Ergebnislisten anzeigen und filtern sowie Details zu einem Ergebnis anzeigen. Weitere Informationen finden Sie unter Überprüfen der Suchdetails und des Suchverlaufs in Security Hub CSPM im AWS Security Hub Benutzerhandbuch. Sie können die Ergebnisse auch automatisch aktualisieren oder sie an eine benutzerdefinierte Aktion senden. Weitere Informationen finden Sie im AWS Security

Hub Benutzerhandbuch unter Automatisches Ändern der Ergebnisse von Security Hub CSPM und Ergreifen von Maßnahmen dazu.

Alle Ergebnisse in Security Hub CSPM verwenden ein standardmäßiges JSON-Format, das AWS Security Finding Format (ASFF). Das ASFF enthält Einzelheiten zur Ursache des Sicherheitsproblems, zu den betroffenen Ressourcen und zum aktuellen Stand der Ergebnisse. Weitere Informationen finden Sie unter AWS -Security Finding-Format (ASFF) im AWS Security Hub - Benutzerhandbuch.

Die DNS-Firewall ist eine der Firewalls AWS-Services , die Ergebnisse an Security Hub CSPM sendet.

Arten von Ergebnissen, die die DNS-Firewall sendet

Die DNS-Firewall verfügt über die folgenden Integrationen:

- Verwaltete Domänenlisten: Sicherheitsfeststellungen im Zusammenhang mit blockierten Abfragen oder Warnmeldungen für Domänen, die AWS verwalteten Domänenlisten zugeordnet sind.
- Benutzerdefinierte Domainlisten: Sicherheitslücken im Zusammenhang mit blockierten Anfragen oder Benachrichtigungen für Domains, die mit der Domainliste des Kunden verknüpft sind.
- DNS Firewall Advanced: Sicherheitsfeststellungen im Zusammenhang mit Anfragen, die von DNS Firewall Advanced blockiert wurden oder bei denen eine Warnung ausgelöst wurde.

Security Hub CSPM nimmt die Ergebnisse der DNS-Firewall im AWS Security Finding Format (ASFF) auf. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an. Die Ergebnisse der DNS-Firewall können die folgenden Werte für haben. `Types`

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Wiederholter Versuch, wenn Security Hub CSPM nicht verfügbar ist

Wenn Security Hub CSPM nicht verfügbar ist, versucht die DNS-Firewall erneut, die Ergebnisse zu senden, bis sie empfangen werden.

Aktualisierung vorhandener Ergebnisse in Security Hub CSPM

Die DNS-Firewall aktualisiert die vorhandenen Ergebnisse, wenn derselbe Befund erneut beobachtet wird.

Typischer Befund aus der DNS-Firewall

Security Hub CSPM nimmt DNS-Firewall-Ergebnisse im AWS Security Finding Format (ASFF) auf.

Hier ist ein Beispiel für ein typisches Ergebnis der DNS-Firewall in ASFF.


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "00000000-0000-0000-0000-example1",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-
resolver-dns-firewall-aws-list",
            "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
            "CompanyName": "Amazon",
            "Region": "us-east-1",
            "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-
rule-group/rslvr-frg-example1",
            "AwsAccountId": "000000000000",
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ],
            "FirstObservedAt": "2024-12-06T19:58:49.000Z",
            "LastObservedAt": "2024-12-06T19:58:49.000Z",
            "CreatedAt": "2024-12-06T19:58:49.000Z",
            "UpdatedAt": "2024-12-06T19:58:49.000Z",
            "Severity": {
                "Label": "HIGH",
                "Normalized": 70
            },
            "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC
 vpc-example1",
            "Description": "DNS Firewall ALERT",
            "ProductFields": {
                "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
                "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-
example1",
                "aws/route53resolver/dnsfirewall/queryType": "A",
                "aws/route53resolver/dnsfirewall/queryClass": "IN",
                "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-
example1",
                "aws/route53resolver/dnsfirewall/transport": "UDP",
                "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
```

```
                "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
List",
                "aws/securityhub/CompanyName": "Amazon"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "rslvr-in-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "ResourceType": "ResolverEndpoint",
                            "EndpointId": "rslvr-in-example1"
                        }
                    }
                },
                {
                    "Type": "Other",
                    "Id": "rni-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "NetworkInterfaceId": "rni-example1",
                            "ResourceType": "ResolverNetworkInterface"
                        }
                    }
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "HIGH"
                },
                "Types": [
                    "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
                ]
            },
            "ProcessedAt": "2024-12-11T19:33:35.494Z"
```

```
        }
```

Aktivieren und Konfigurieren der Integration

Um die DNS-Firewall in Security Hub CSPM zu integrieren, müssen Sie zuerst Security Hub CSPM aktivieren. Informationen zur Aktivierung von Security Hub CSPM finden Sie unter Enabling Security Hub CSPM im Benutzerhandbuch.AWS Security Hub

Einstellung der Übermittlung der Ergebnisse an Security Hub CSPM

Um das Senden von DNS-Firewall-Ergebnissen an Security Hub CSPM zu beenden, können Sie die Security Hub CSPM-Konsole oder die Security Hub CSPM-API verwenden.

Anweisungen finden Sie im Benutzerhandbuch unter Deaktivierung des Flusses von Ergebnissen aus einer Integration.AWS Security Hub

Amazon Route 53 überwachen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. Aber bevor Sie mit der Überwachung beginnen, sollten Sie einen Überwachungsplan mit Antworten auf die folgenden Fragen erstellen:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Themen

Öffentliche DNS-Abfrageprotokollierung

Sie können Amazon Route 53 so konfigurieren, dass Informationen zu den öffentlichen DNS-Abfragen protokolliert werden, die Route 53 empfängt, z. B. die folgenden:

- Domain oder Subdomain, die angefordert wurde

- Das Datum und die Uhrzeit der Anforderung
- DNS-Datensatztyp (z. B. A oder AAAA)
- Der Edge-Standort von Route 53, der auf die DNS-Abfrage geantwortet hat
- Der DNS-Antwortcode, wie z. B. `NoError` oder `ServFail`

Sobald Sie die Abfrageprotokollierung konfiguriert haben, sendet Route 53 CloudWatch Protokolle an Logs. Sie verwenden CloudWatch Logs-Tools, um auf die Abfrageprotokolle zuzugreifen.

Abfrageprotokolle enthalten nur die Abfragen, die DNS-Resolver an Route 53 senden. Wenn ein DNS-Resolver die Antwort auf eine Anfrage bereits zwischengespeichert hat (z. B. die IP-Adresse für einen Load Balancer, z. B. .com), gibt der Resolver weiterhin die zwischengespeicherte Antwort zurück, ohne die Abfrage an Route 53 zu senden, bis die TTL für den entsprechenden Datensatz abläuft.

Abhängig davon, wie viele DNS-Abfragen für einen Domainnamen (example.com) oder Subdomainnamen (www.example.com) übermittelt werden, welche Auflöser von Ihren Benutzern verwendet werden und welche TTL für den Datensatz gilt, enthalten die Abfrageprotokolle möglicherweise Informationen zu nur einer von mehreren tausend Abfragen, die an DNS-Auflöser übermittelt wurden. Weitere Information zur Funktionsweise von DNS finden Sie unter Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird.

Wenn Sie keine detaillierten Protokollierungsinformationen benötigen, können Sie mithilfe von CloudWatch Amazon-Metriken die Gesamtzahl der DNS-Abfragen ermitteln, auf die Route 53 für eine gehostete Zone antwortet. Weitere Informationen finden Sie unter Anzeigen von DNS-Abfragemetriken für eine öffentliche gehostete Zone.

Themen

Konfigurieren der Protokollierung für DNS-Abfragen

Um die Protokollierung von DNS-Abfragen für eine bestimmte gehostete Zone zu starten, führen Sie die folgenden Aufgaben in der Amazon-Route 53-Konsole aus:

- Wählen Sie die CloudWatch Logs-Protokollgruppe aus, in der Route 53 Protokolle veröffentlichen soll, oder erstellen Sie eine neue Protokollgruppe.

  > **Note**
  >
  > Die Lambda-Funktion muss sich in der Region USA Ost (Nord-Virginia) befinden.

- Wählen Sie Erstellen aus, um den Vorgang abzuschließen.

> **Note**
>
> Wenn Benutzer DNS-Abfragen für Ihre Domain übermitteln, sollten Ihnen wenige Minuten nach Erstellung der Konfiguration für die Abfrageprotokollierung Abfragen in den Protokollen angezeigt werden.

So konfigurieren Sie die Protokollierung für DNS-Abfragen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie die gehostete Zone aus, für die Sie die Abfrageprotokollierung konfigurieren möchten.
4. Wählen Sie im Bereich Hosted zone details Configure query logging.
5. Wählen Sie eine vorhandene Protokollgruppe aus, oder erstellen Sie eine neue Protokollgruppe.
6. Wenn Sie eine Warnung zu Berechtigungen erhalten (dies geschieht, wenn Sie die Abfrageprotokollierung noch nicht mit der neuen Konsole konfiguriert haben), führen Sie einen der folgenden Schritte aus:

   - Wenn Sie bereits 10 Ressourcenrichtlinien haben, können Sie nicht mehr erstellen. Wählen Sie eine Ihrer Ressourcenrichtlinien aus und wählen SieBearbeitenaus. Die Bearbeitung gewährt Route 53 Berechtigungen zum Schreiben von Protokollen in Ihre Protokollgruppen.

Wählen Sie Speichern. Der Alarm verschwindet, und Sie können mit dem nächsten Schritt fortfahren.

- Wenn Sie die Abfrageprotokollierung noch nie konfiguriert haben (oder wenn Sie noch nicht 10 Ressourcenrichtlinien erstellt haben), müssen Sie Route 53 Berechtigungen zum Schreiben von Protokollen in Ihre CloudWatch Logs-Gruppen erteilen. Klicken Sie aufGewähren von Berechtigungenaus. Der Alarm verschwindet, und Sie können mit dem nächsten Schritt fortfahren.

7. Wählen Sie Berechtigungen — optional, um eine Tabelle aufzurufen, aus der hervorgeht, ob die Ressourcenrichtlinie mit der CloudWatch Protokollgruppe übereinstimmt und ob Route 53 berechtigt ist, Protokolle zu veröffentlichen CloudWatch.
8. Wählen Sie Erstellen aus.

Amazon CloudWatch für den Zugriff auf DNS-Abfrageprotokolle verwenden

Amazon Route 53 sendet Abfrageprotokolle direkt an CloudWatch Logs; auf die Protokolle kann nie über Route 53 zugegriffen werden. Stattdessen verwenden Sie Logs, um CloudWatch Logs nahezu in Echtzeit anzusehen, Daten zu suchen und zu filtern und Logs nach Amazon S3 zu exportieren.

Route 53 erstellt für jeden Route 53-Edge-Standort einen CloudWatch Logs-Log-Stream, der auf DNS-Anfragen für die angegebene Hosting-Zone reagiert und Abfrageprotokolle an den entsprechenden Log-Stream sendet. Das Format für den Namen jedes Protokollstreams ist*hosted-zone-id*/*edge-location-ID*, zum BeispielZ1D633PJN98FT9/DFW3.

Jede Kantenposition wird durch einen aus drei Buchstaben bestehenden Code und eine willkürlich zugewiesene Zahl identifiziert, z. B. DFW3 Der Code aus drei Buchstaben entspricht dem Code der International Air Transport Association für einen Flughafen in der Nähe des Edge-Standorts. (Diese Abkürzungen ändern sich möglicherweise in der Zukunft.) Eine Liste der Edge-Standorte finden Sie unter „Das globale Route 53-Netzwerk“ auf der Seite mit den Route 53-Produktdetails.

> **Note**
>
> Möglicherweise sehen Sie einige Präfixe oder Suffixe, die nicht der obigen Konvention entsprechen. Diese kodieren Attribute, die nur für den internen Gebrauch bestimmt sind.

Weitere Informationen finden Sie in der entsprechenden Dokumentation:

- Amazon CloudWatch Logs-Benutzerhandbuch

- Amazon CloudWatch Logs API-Referenz
- CloudWatch Abschnitt „Logs“ der AWS CLI Befehlsreferenz
- Werte in DNS-Abfrageprotokollen

Ändern des Aufbewahrungszeitraums für Protokolle und Exportieren von Protokollen zu Amazon S3

Standardmäßig speichert CloudWatch Logs Abfrageprotokolle auf unbestimmte Zeit. Sie können optional einen Aufbewahrungszeitraum angeben, sodass CloudWatch Logs Protokolle löscht, die älter als der Aufbewahrungszeitraum sind. Weitere Informationen finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs im CloudWatch Amazon-Benutzerhandbuch.

Wenn Sie Protokolldaten behalten möchten, aber keine CloudWatch Logs-Tools zum Anzeigen und Analysieren der Daten benötigen, können Sie Protokolle nach Amazon S3 exportieren, wodurch Ihre Speicherkosten gesenkt werden können. Weitere Informationen finden Sie unter Exportieren von Protokolldaten zu Amazon S3.

Informationen zu Preisen finden Sie auf der entsprechenden Seite mit den Preisen:

- „Amazon CloudWatch Logs“ auf der CloudWatch Preisseite
- Amazon S3 – Preise

> **Note**
>
> Wenn Sie Route 53 für die Protokollierung von DNS-Abfragen konfigurieren, fallen keine -Gebühren an.

Anhalten der Abfrageprotokollierung

Wenn Sie möchten, dass Amazon Route 53 keine Abfrageprotokolle mehr an Logs sendet, gehen Sie wie folgt vor, um die Konfiguration der Abfrageprotokollierung zu löschen. CloudWatch

So löschen Sie eine Konfiguration für die Abfrageprotokollierung

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie das Optionsfeld (nicht den Namen) für die gehostete Zone aus, für die Sie die Konfiguration für die Abfrageprotokollierung löschen möchten.
4. Wählen Sie im Bereich Hosted zone details Configure query logging.
5. Wählen Sie zur Bestätigung Delete.

Werte in DNS-Abfrageprotokollen

Jede Protokolldatei enthält einen einzelnen Protokolleintrag für jede DNS-Abfrage, die Amazon Route 53 von DNS-Resolvern am entsprechenden Edge-Standort erhalten hat. Jeder Protokolleintrag enthält die folgenden Werte:

Protokollformatversion

Die Versionsnummer dieses Abfrageprotokolls. Wenn dem Protokoll Felder hinzugefügt werden oder das Format vorhandener Felder geändert wird, wird dieser Wert erhöht.

Abfragezeitstempel

Das Datum und die Uhrzeit, an dem/zu der Route 53 auf die Anforderung geantwortet hat; im ISO 8601-Format und in koordinierter Weltzeit (Coordinated Universal Time, UTC), z. B. `2017-03-16T19:20:25.177Z`.

Informationen zum ISO 8601-Format finden Sie im Wikipedia-Artikel ISO 8601. Informationen zu UTC finden Sie im Wikipedia-Artikel Coordinated Universal Time.

ID der gehosteten Zone

Die ID der gehosteten Zone, die mit allen DNS-Abfragen in diesem Protokoll verknüpft ist.

Abfragename

Die Domain oder Subdomain, die in der Anfrage angegeben wurde.

Abfragetyp

Entweder der DNS-Datensatztyp, der in der Anfrage angegeben wurde, oder `ANY`. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

Antwortcode

Der DNS-Antwortcode, den Route 53 als Antwort auf die DNS-Abfrage zurückgegeben hat.

Layer 4-Protokoll

Das Protokoll, das zum Übermitteln der Abfrage verwendet wurde, entweder TCP oder UDP.

Route-53-Edge-Standort

Der Route 53-Edge-Standort, der auf die Abfrage geantwortet hat. Jede Edge-Position wird durch einen aus drei Buchstaben bestehenden Code und eine beliebige Zahl identifiziert, DFW3 z. B. Der Code aus drei Buchstaben entspricht dem Code der International Air Transport Association für einen Flughafen in der Nähe des Edge-Standorts. (Diese Abkürzungen ändern sich möglicherweise in der Zukunft.)

Eine Liste der Edge-Standorte finden Sie unter „Das globale Route 53-Netzwerk“ auf der Seite mit den Route 53-Produktdetails.

Resolver-IP-Adresse

Die IP-Adresse des DNS-Auflösers, der die Anfrage an Route 53 übermittelt hat.

EDNS-Client-Subnetz

Eine teilweise IP-Adresse für den Client, von dem die Anfrage gesendet wurde, wenn über den DNS-Auflöser verfügbar.

Weitere Informationen finden Sie im IETF-Entwurf Client-Subnetz in DNS-Anfragen.

Beispiel für ein Abfrageprotokoll:

Ein Beispiel für ein Abfrageprotokoll (Region ist ein Platzhalter):

```
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 -
```

Abfrageprotokollierung

Sie können die folgenden DNS-Abfragen protokollieren:

- Abfragen, die ihren Ursprung in Amazon Virtual Private Cloud haben, VPCs die Sie angeben, sowie die Antworten auf diese DNS-Abfragen.
- Abfragen von On-Premises-Ressourcen, die einen eingehenden Resolver-Endpunkt verwenden.
- Abfragen, die einen ausgehenden Resolver-Endpunkt für rekursive DNS-Auflösung verwenden.
- Abfragen, die Resolver DNS-Firewall-Regeln verwenden, um Domainlisten zu blockieren, zuzulassen oder zu überwachen.

Die VPC Resolver-Abfrageprotokolle enthalten Werte wie die folgenden:

- Die AWS Region, in der die VPC erstellt wurde
- Die ID des VPC, aus dem die Abfrage stammt
- Die IP-Adresse der Instance, von der die Abfrage stammt
- Die Instance-ID der Ressource, von der die Abfrage stammt
- Das Datum und die Uhrzeit, als die Abfrage zum ersten Mal durchgeführt wurde
- Der angeforderte DNS-Name (z. B. prod.example.com)
- Der DNS-Datensatztyp (z. B. A oder AAAA)
- Der DNS-Antwortcode, z. B. `NoError` oder `ServFail`
- Die DNS-Antwortdaten, z. B. die IP-Adresse, die als Antwort auf die DNS-Abfrage zurückgegeben wird
- Eine Antwort auf eine DNS-Firewall-Regelaktion

Eine detaillierte Liste aller protokollierten Werte und ein Beispiel finden Sie unterWerte, die in den VPC Resolver-Abfrageprotokollen erscheinenaus.

> **Note**
>
> Wie bei DNS-Resolvern üblich, speichern Resolver DNS-Abfragen für einen Zeitraum im Cache, der durch die time-to-live (TTL) für den Resolver bestimmt wird. Der Route 53 VPC Resolver speichert Anfragen, die von Ihrem stammen, im Cache und beantwortet VPCs, wann immer möglich, aus dem Cache, um die Antworten zu beschleunigen. Die VPC

Resolver-Abfrageprotokollierung protokolliert nur eindeutige Abfragen, keine Abfragen, auf die VPC Resolver aus dem Cache antworten kann.
Nehmen wir zum Beispiel an, dass eine EC2 Instanz in einer der Instanzen VPCs , für die eine Abfrageprotokollierungskonfiguration Abfragen protokolliert, eine Anfrage an accounting.example.com sendet. VPC Resolver speichert die Antwort auf diese Abfrage im Cache und protokolliert die Abfrage. Wenn die elastic network interface derselben Instance innerhalb der TTL des VPC Resolver-Caches eine Abfrage nach accounting.example.com durchführt, antwortet VPC Resolver auf die Abfrage aus dem Cache. Die zweite Abfrage wird nicht protokolliert.

Sie können die Protokolle an eine der folgenden Ressourcen senden: AWS

- Amazon CloudWatch Logs (CloudWatch Logs) -Protokollgruppe
- Amazon-S3-Bucket.
- Firehose-Bereitstellungsdat

Weitere Informationen finden Sie unter AWS Ressourcen, an die Sie VPC Resolver-Abfrageprotokolle senden können.

Themen

AWS Ressourcen, an die Sie VPC Resolver-Abfrageprotokolle senden können

Note

Wenn Sie erwarten, Abfragen für Workloads mit hohen Abfragen pro Sekunde (QPS) zu protokollieren, sollten Sie Amazon S3 verwenden, um sicherzustellen, dass Ihre Abfrageprotokolle beim Schreiben an Ihr Ziel nicht eingeschränkt werden. Wenn Sie Amazon verwenden CloudWatch, können Sie Ihr Limit für Anfragen pro Sekunde für den `PutLogEvents` Vorgang erhöhen. Weitere Informationen zur Erhöhung Ihrer

CloudWatch Limits finden Sie unter CloudWatch Log-Kontingente im CloudWatch Amazon-Benutzerhandbuch.

Sie können VPC Resolver-Abfrageprotokolle an die folgenden AWS Ressourcen senden:

Amazon CloudWatch Logs (Amazon CloudWatch Logs) -Protokollgruppe

Sie können Protokolle mit Logs Insights analysieren und Metriken und Alarme erstellen.

Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Amazon-S3-Bucket.

Das Speichern von Protokollen in einem S3-Bucket ist bei der langfristigen Protokollarchivierung wirtschaftlich. Die Latenz ist normalerweise höher.

Alle serverseitigen S3-Verschlüsselungsoptionen werden unterstützt. Weitere Informationen finden Sie unter Schützen von Daten mit serverseitiger Verschlüsselung im Amazon-S3-Entwicklerhandbuch.

Wenn Sie sich für serverseitige Verschlüsselung mit AWS KMS Schlüsseln (SSE-KMS) entscheiden, müssen Sie die Schlüsselrichtlinie für Ihren vom Kunden verwalteten Schlüssel aktualisieren, damit das Konto für die Protokollzustellung in Ihren Amazon S3 S3-Bucket schreiben kann. Weitere Informationen zur erforderlichen Schlüsselrichtlinie für die Verwendung mit SSE-KMS finden Sie unter serverseitige Verschlüsselung des Amazon S3 S3-Buckets im CloudWatch Amazon-Benutzerhandbuch.

Wenn sich der S3-Bucket in einem Konto befindet, das Ihnen gehört, werden die erforderlichen Berechtigungen automatisch Ihrer Bucket-Richtlinie hinzugefügt. Wenn Sie Protokolle an einen S3-Bucket in einem Konto senden möchten, das Sie nicht besitzen, muss der Besitzer des S3-Buckets Berechtigungen für Ihr Konto in seiner Bucket-Richtlinie hinzufügen. Zum Beispiel:

JSON

```
{
    "Version":"2012-10-17",
    "Id": "CrossAccountAccess",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your_bucket_name/
AWSLogs/your_caller_account/*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
}
```

> **Note**
>
> Wenn Sie Protokolle in einem zentralen S3-Bucket für Ihre Organisation speichern möchten, sollten Sie die Konfiguration der Abfrageprotokollierung über ein zentralisiertes Konto (mit den erforderlichen Berechtigungen zum Schreiben in einen zentralen Bucket) einrichten undRAM, um die Konfiguration über Konten hinweg freizugeben.

Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Simple Storage Service.

Firehose-Bereitstellungsdat

Sie können Protokolle in Echtzeit an Amazon OpenSearch Service, Amazon Redshift oder andere Anwendungen streamen.

Weitere Informationen finden Sie im Amazon Data Firehose Developer Guide.

Informationen zu den Preisen für die Resolver-Abfrageprotokollierung finden Sie unter CloudWatch Amazon-Preise.

CloudWatch Bei der Verwendung von VPC Resolver-Protokollen fallen Gebühren für Vending Logs an, auch wenn Protokolle direkt in Amazon S3 veröffentlicht werden. Weitere Informationen finden Sie unter Preise für Logs bei Amazon CloudWatch .

Konfigurationen für die Protokollierung von Resolver-Abfragen verwalten

Konfiguration (VPC Resolver-Abfrageprotokollierung)

Sie können die VPC Resolver-Abfrageprotokollierung auf zwei Arten konfigurieren:

- Direkte VPC-Zuordnung — VPCs Direkter Zugriff auf eine Konfiguration zur Abfrageprotokollierung.
- Profilzuordnung — Ordnen Sie eine Abfrageprotokollierungskonfiguration einem Route 53 53-Profil zu, wodurch die Protokollierung auf alle mit diesem Profil VPCs verknüpften Profile angewendet wird. Weitere Informationen finden Sie unter Ordnen Sie die Konfigurationen der VPC Resolver-Abfrageprotokollierung einem Route 53 53-Profil zu.

Um mit der Protokollierung von DNS-Abfragen zu beginnen, die ihren Ursprung in Ihrem haben VPCs, führen Sie die folgenden Aufgaben in der Amazon Route 53-Konsole aus:

So konfigurieren Sie die Protokollierung der Resolver-Abfrage

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Erweitern Sie das Route-53-Konsolenmenü. Wählen Sie oben links in der Konsole die drei horizontalen Balken

   (☰)

   aus.
3. Wählen Sie im Resolver-Menü die Option Abfrageprotokollierung.
4. Wählen Sie in der Regionsauswahl die AWS Region aus, in der Sie die Konfiguration für die Abfrageprotokollierung erstellen möchten. Dies muss dieselbe Region sein, in der Sie die Region erstellt haben VPCs , für die Sie DNS-Abfragen protokollieren möchten. Wenn Sie VPCs in mehreren Regionen arbeiten, müssen Sie mindestens eine Konfiguration für die Abfrageprotokollierung für jede Region erstellen.

5. Wählen Sie Konfigurieren der Abfrageprotokollierung.
6. Geben Sie die folgenden Werte an:

   Name der Abfrageprotokollierungskonfiguration

   Geben Sie einen Namen für Ihre Abfrageprotokollierungskonfiguration ein. Der Name wird in der Konsole in der Liste der Konfigurationen für die Abfrageprotokollierung angezeigt. Geben Sie einen Namen ein, den Sie später bei der Suche nach dieser Konfiguration unterstützen.

   Ziel der Abfrageprotokolle

   Wählen Sie den AWS Ressourcentyp aus, an den VPC Resolver Abfrageprotokolle senden soll. Informationen zur Auswahl zwischen den Optionen (CloudWatch Logs-Protokollgruppe, S3-Bucket und Firehose-Lieferstream) finden Sie unterAWS Ressourcen, an die Sie VPC Resolver-Abfrageprotokolle senden können.

   Nachdem Sie den Ressourcentyp ausgewählt haben, können Sie entweder eine weitere Ressource dieses Typs erstellen oder eine vorhandene Ressource auswählen, die mit dem aktuellen AWS Konto erstellt wurde.

   > **Note**
   >
   > Sie können nur Ressourcen auswählen, die in der AWS -Region erstellt wurden, die Sie in Schritt 4 ausgewählt haben, der Region, in der Sie die Abfrageprotokollierungskonfiguration erstellen. Wenn Sie eine neue Ressource erstellen, wird diese Ressource in derselben Region erstellt.

   VPCs um Abfragen zu protokollieren für

   Bei dieser Konfiguration für die Abfrageprotokollierung werden DNS-Abfragen protokolliert, die ihren Ursprung in der VPCs von Ihnen ausgewählten Datei haben. Aktivieren Sie das Kontrollkästchen für jede VPC in der aktuellen Region, für die VPC Resolver Abfragen protokollieren soll, und wählen Sie dann Wählen aus.

   Alternative: Anstatt eine VPCs direkte Zuordnung vorzunehmen, können Sie diese Abfrageprotokollierungskonfiguration einem Route 53 53-Profil zuordnen, wodurch die Protokollierung auf alle mit diesem Profil VPCs verknüpften Daten angewendet wird.

Weitere Informationen finden Sie unter Ordnen Sie die Konfigurationen der VPC Resolver-Abfrageprotokollierung einem Route 53 53-Profil zu.

> **Note**
>
> Die VPC Protokollzustellung kann für einen bestimmten Zieltyp nur einmal aktiviert werden. Die Protokolle können nicht an mehrere Ziele desselben Typs übermittelt werden. Beispielsweise können VPC Protokolle nicht an zwei Amazon S3 Ziele übermittelt werden.

7. Wählen Sie Konfigurieren der Abfrageprotokollierung aus.

> **Note**
>
> Sie sollten innerhalb weniger Minuten nach erfolgreicher Erstellung der Konfiguration für die Abfrageprotokollierung DNS-Abfragen von Ressourcen in Ihrer VPC in den Protokollen anzeigen.

Werte, die in den VPC Resolver-Abfrageprotokollen erscheinen

Jede Protokolldatei enthält einen einzelnen Protokolleintrag für jede DNS-Abfrage, die Amazon Route 53 von DNS-Resolvern am entsprechenden Edge-Standort erhalten hat. Jeder Protokolleintrag enthält die folgenden Werte:

version

Die Versionsnummer dieses Abfrageprotokolls. Die aktuelle Version ist `1.1`.

Der Versions-Schlüsselwert enthält eine Haupt- und eine Nebenversion im Format **`major_version.minor_version`**.. Sie können beispielsweise ein `version`-Wert`1.7`, wobei `1` die Hauptversion ist, und 7 die Nebenversion.

Die Hauptversion wird erhöht, wenn Route 53 eine Änderung an der Ereignisstruktur vornimmt, die nicht abwärtskompatibel ist. Dies beinhaltet das Entfernen eines JSON-Feldes, das bereits vorhanden ist, oder das Ändern, wie die Inhalte eines Feldes dargestellt werden (Beispiel: ein Datumsformat).

Route 53 erhöht die Nebenversion, wenn eine Änderung der Protokolldatei neue Felder hinzufügt. Dies kann auftreten, wenn neue Informationen für einige oder alle vorhandenen DNS-Abfragen innerhalb einer VPC verfügbar sind.

account_id

Die ID des AWS Kontos, das die VPC erstellt hat.

Region

Die AWS Region, in der Sie die VPC erstellt haben.

vpc_id

Die ID der VPC, in der die Abfrage stammt.

query_timestamp

Das Datum und die Uhrzeit, an dem/zu der auf die Anforderung geantwortet hat; im ISO 8601-Format und in koordinierter Weltzeit (Coordinated Universal Time, UTC), z. B. `2017-03-16T19:20:177Z`.

Informationen zum ISO 8601-Format finden Sie im Wikipedia-Artikel ISO 8601. Informationen zu UTC finden Sie im Wikipedia-Artikel Coordinated Universal Time.

query_name

Der Domainnamen (example.com) oder Subdomainname (www.example.com), der in der Abfrage angegeben wurde.

query_type

Entweder der DNS-Datensatztyp, der in der Anfrage angegeben wurde, oder `ANY`. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

query_class

Die ID der Abfrage.

rcode

Der DNS-Antwortcode, den VPC Resolver als Antwort auf die DNS-Anfrage zurückgegeben hat. Ein Code, der angibt, ob die Abfrage gültig war oder nicht. Der gängigste Antwortcode ist `NOERROR` und bedeutet, dass die Abfrage gültig war. Wenn die Antwort nicht gültig ist, gibt Resolver einen Antwortcode mit Erklärung aus. Eine Liste möglicher Antwortcodes finden Sie unter DNS RCODEs auf der IANA-Website.

Antwort_Typ

Der DNS-Eintragstyp (z. B. A, MX oder CNAME) des Werts, den VPC Resolver als Antwort auf die Abfrage zurückgibt. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

rdata

Der Wert, den VPC Resolver als Antwort auf die Abfrage zurückgegeben hat. Für einen A-Datensatz ist dies beispielsweise eine IP-Adresse im IPv4 Format. Für einen CNAME-Datensatz ist dies der Domainname im CNAME-Datensatz.

Antwort_Klasse

Die Klasse der VPC-Resolver-Antwort auf die Abfrage.

srcaddr

IP-Adresse des Hosts, von dem die Anfrage stammt.

srcport

Der Port auf der Instance, von der die Abfrage stammt.

Transport

Das Protokoll, das zum Senden der DNS-Abfrage verwendet wird.

srcids

IDs von dem`instance`, und dem`resolver_endpoint`, von dem `resolver_network_interface` die DNS-Abfrage stammt oder über die die DNS-Anfrage weitergeleitet wurde.

Instance

Die ID der Instance, von der die Abfrage stammt.

> **Note**
>
> Wenn Sie in den Route 53 VPC Resolver-Abfrageprotokollen eine Instance-ID sehen, die in Ihrem Konto nicht sichtbar ist, kann das daran liegen, dass die DNS-Abfrage entweder AWS CloudShell von der Amazon EKS- oder der Fargate-Konsole stammt, die von Ihnen verwendet wurde. AWS Lambda

resolver_endpoint

Die ID des Auflösungsendpunkts, der die DNS-Abfrage an On-Premises-DNS-Server weiterleitet.

> **Note**
>
> Wenn Sie CNAME-Einträge haben, die über verschiedene Weiterleitungsregeln mit unterschiedlichen Resolver-Endpunkten verknüpft sind, zeigen Abfrageprotokolle nur die ID des letzten Resolver-Endpunkts an, der in der Kette verwendet wurde. Um den gesamten Lösungspfad über mehrere Endpunkte hinweg nachzuverfolgen, können Sie die Protokolle verschiedener Konfigurationen der Abfrageprotokollierung korrelieren.

firewall_rule_group_id

Die ID des DNS-Firewall-Regelgruppe, die dem Domainnamen in der Abfrage entspricht. Diese Option wird nur aufgefüllt, wenn die DNS-Firewall eine Übereinstimmung für eine Regel gefunden hat, deren Aktion auf Warnung oder Blockierung festgelegt ist.

Weitere Informationen zu Firewll-Regelgruppen finden Sie in der DNS-Firewall-Regelgruppen und -Regeln.

firewall_rule_action

Die Aktion, die von der Regel angegeben wurde, die dem Domainnamen in der Abfrage entspricht. Diese Option wird nur aufgefüllt, wenn die DNS-Firewall eine Übereinstimmung für eine Regel gefunden hat, deren Aktion auf Warnung oder Blockierung festgelegt ist.

Firewall_domain_list_id

Die Domainliste, die von der Regel verwendet wurde, die dem Domainnamen in der Abfrage entspricht. Diese Option wird nur aufgefüllt, wenn die DNS-Firewall eine Übereinstimmung für eine Regel gefunden hat, deren Aktion auf Warnung oder Blockierung festgelegt ist.

additional_properties

Zusätzliche Informationen zu den Protokollübermittlungsereignissen. is_delayed: Wenn es zu einer Verzögerung bei der Übermittlung der Protokolle kommt.

Beispiel für das Route 53 VPC Resolver-Abfrageprotokoll

Hier ist ein Beispiel für ein Resolver-Abfrageprotokoll:

```
    {
      "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"
  }
```


Konfiguration der Resolver-Abfrageprotokollierung mit anderen Konten teilen AWS

Sie können die Konfigurationen für die Abfrageprotokollierung, die Sie mit einem AWS Konto erstellt haben, mit anderen AWS Konten teilen. Um Konfigurationen gemeinsam zu nutzen, ist die Route 53 VPC Resolver-Konsole in AWS Resource Access Manager integriert. Weitere Informationen zu Resource Access Manager finden Sie im Benutzerhandbuch zu Resource Access Manager.

Beachten Sie Folgendes:

Zuordnen zu gemeinsam genutzten Konfigurationen für die VPCs Abfrageprotokollierung

Wenn ein anderes AWS Konto eine oder mehrere Konfigurationen mit Ihrem Konto gemeinsam genutzt hat, können Sie diese Konfiguration genauso zuordnen VPCs wie Konfigurationen, die Sie selbst erstellt haben. VPCs

Löschen oder Aufheben der Freigabe einer Konfiguration

Wenn Sie eine Konfiguration mit anderen Konten teilen und dann entweder die Konfiguration löschen oder die gemeinsame Nutzung beenden und wenn eine oder mehrere mit der Konfiguration verknüpft VPCs waren, beendet Route 53 VPC Resolver die Protokollierung von DNS-Abfragen, die ihren Ursprung in diesen Konten haben. VPCs

Maximale Anzahl von Konfigurationen für die Abfrageprotokollierung VPCs , die einer Konfiguration zugeordnet werden können

Wenn ein Konto eine Konfiguration erstellt und sie mit einem oder mehreren anderen Konten gemeinsam nutzt, wird die maximale Anzahl davon VPCs , die der Konfiguration zugeordnet werden kann, pro Konto angewendet. Wenn Sie beispielsweise 10.000 Konten in Ihrer Organisation haben, können Sie die Konfiguration für die Abfrageprotokollierung im zentralen Konto erstellen und sie über teilen, AWS RAM um sie für die Organisationskonten freizugeben. Die Organisationskonten verknüpfen die Konfiguration dann damit, dass sie sie VPCs anhand der VPC-Zuordnungen für die Abfrageprotokollkonfiguration ihres Kontos pro AWS-Region Limit von 100 zählen. Wenn sich jedoch alle in einem einzigen Konto VPCs befinden, müssen die Dienstlimits des Kontos möglicherweise erhöht werden.

Aktuelle VPC-Resolver-Kontingente finden Sie unter. Kontingente auf Route 53 VPC Resolver

Berechtigungen

Um eine Regel mit einem anderen AWS Konto zu teilen, benötigen Sie die Berechtigung, die PutResolverQueryLogConfigPolicyAktion zu verwenden.

Einschränkungen für das AWS Konto, mit dem eine Regel geteilt wird

Das Konto, für das eine Regel freigegeben werden, kann die Regel nicht ändern oder löschen.

Tagging

Nur das Konto, das eine Regel erstellt hat, kann Tags zu dieser hinzufügen, löschen oder anzeigen.

Führen Sie die folgenden Schritte aus, um den aktuellen Freigabestatus einer Regel (einschließlich des Kontos, das die Regel freigegeben hat, oder des Kontos, für das eine Regel freigegeben wurde) anzuzeigen und um Regeln für ein anderes Konto freizugeben.

So zeigen Sie den Freigabestatus an und geben Abfrageprotokolle mit einem anderen AWS -Konto frei

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich die Option Query Editor (Abfrage-Editor) aus.
3. Wählen Sie in der Navigationsleiste die Region aus, in der Sie die Regel erstellt haben.

   Die Spalte Sharing status (Freigabestatus) zeigt den aktuellen Freigabestatus der Regeln, die von dem aktuellen Konto erstellt wurden oder die für das aktuelle Konto freigegeben wurden:

   - Nicht geteilt: Das aktuelle AWS Konto hat die Regel erstellt, und die Regel wird nicht mit anderen Konten geteilt.
   - Shared by me (Von mir freigegeben): Das aktuelle Konto hat die Regel erstellt und für ein oder mehrere Konten freigegeben.
   - Shared with me (Für mich freigegeben): Ein anderes Konto hat die Regel erstellt und für das aktuelle Konto freigegeben.
4. Wählen Sie den Namen der Regel, für die Sie Freigabeinformationen anzeigen möchten oder die Sie für ein anderes Konto freigeben möchten.

   Auf der *`rule name`* Seite Regel: zeigt der Wert unter Besitzer die ID des Kontos an, mit dem die Regel erstellt wurde. Dies ist das aktuelle Konto, sofern der Wert unter Sharing Status (Freigabestatus) nicht Shared with me (Für mich freigegeben) lautet. In diesem Fall handelt es sich bei Owner (Eigentümer) um das Konto, das die Regel erstellt und für das aktuelle Konto freigegeben hat.

   Der Freigabestatus wird ebenfalls angezeigt.
5. Wählen Sie Konfiguration teilen, um die AWS RAM Konsole zu öffnen
6. Um eine Ressourcenfreigabe zu erstellen, folgen Sie den Schritten unter Erstellen einer Ressourcenfreigabe AWS RAM im AWS RAM Benutzerhandbuch.

> **Note**
>
> Sie können keine Freigabeeinstellungen aktualisieren. Wenn Sie eine der folgenden Einstellungen ändern möchten, müssen Sie eine Regel mit den neuen Einstellungen freigeben und die alten Freigabeeinstellungen anschließend entfernen.

Überwachung von Domainregistrierungen

Das Amazon Route 53-Dashboard liefert detaillierte Informationen über den Status Ihrer Domainregistrierungen, einschließlich der folgenden:

- Status neuer Domainregistrierungen
- Status von Domainübertragungen in Route 53
- Liste der Domains, die kurz vor dem Ablaufdatum stehen

Wir empfehlen, dass Sie regelmäßig das Dashboard in der Route 53-Konsole überprüfen, vor allem nach der Registrierung einer neuen Domain oder der Übertragung einer Domain in Route 53, um zu bestätigen, dass es keine Probleme gibt.

Außerdem sollten Sie überprüfen, ob die Kontaktinformationen für Ihre Domains auf dem neuesten Stand sind. Wenn das Ablaufdatum für eine Domain naht, senden wir eine E-Mail an den Kontakt für die Domain mit Informationen darüber, wann die Domain abläuft und wie sie verlängert werden kann.

Überwachen Sie Ihre Ressourcen mit Amazon Route 53 Health Checks und Amazon CloudWatch

Sie können Ihre Ressourcen überwachen, indem Sie Amazon Route 53-Zustandsprüfungen erstellen, mit denen Rohdaten gesammelt und CloudWatch zu lesbaren Metriken nahezu in Echtzeit verarbeitet werden. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Ressourcen ausgeführt werden. Standardmäßig werden Metrikdaten für Route 53-Zustandsprüfungen automatisch in Intervallen von einer CloudWatch Minute gesendet.

Weitere Informationen zu Route 53-Zustandsprüfungen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch. Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Metriken und Dimensionen für Route 53-Zustandsprüfungen

Wenn Sie eine Zustandsprüfung erstellen, beginnt Amazon Route 53, einmal pro Minute Metriken und Dimensionen an CloudWatch etwa die von Ihnen angegebene Ressource zu senden. In der Route 53-Konsole können Sie den Status Ihrer Zustandsprüfungen anzeigen. Sie können auch die folgenden Verfahren verwenden, um die Metriken in der CloudWatch Konsole oder mithilfe von AWS Command Line Interface (AWS CLI) anzuzeigen.

So zeigen Sie Metriken mit der CloudWatch Konsole an

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Klicken Sie auf der Registerkarte All Metrics auf Route 53.
4. Wählen Sie Health Check Metrics.

Um Metriken mit dem anzuzeigen AWS CLI

- Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Themen

- CloudWatch Metriken für Route 53-Zustandsprüfungen
- Dimensionen für Route 53-Metriken für Zustandsprüfungen

CloudWatch Metriken für Route 53-Zustandsprüfungen

Der Namespace `AWS/Route53` enthält die folgenden Metriken zu Route 53-Zustandsprüfungen.

ChildHealthCheckHealthyCount

Zur Berechnung einer Zustandsprüfung, die Anzahl der fehlerfreien Zustandsprüfungen.

Gültige Statistiken: Durchschnitt (empfohlen), Minimum, Maximum

Einheiten: Anzahl

ConnectionTime

Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen benötigten, um eine TCP-Verbindung mit dem Endpunkt herzustellen. Sie können `ConnectionTime` für eine Zustandsprüfung für die gesamten Regionen oder für eine ausgewählte geografische Region angezeigt bekommen.

Gültige Statistiken: Durchschnitt (empfohlen), Minimum, Maximum

Einheiten: Millisekunden

HealthCheckPercentageHealthy

Die Prozentzahl von Route 53-Zustandsprüfungen, die den ausgewählten Endpunkt als fehlerfrei betrachten.

Gültige Statistiken: Durchschnitt, Minimum, Maximum

Einheiten: Prozent

HealthCheckStatus

Der Status des Endpunkts für die Integritätsprüfung, der CloudWatch die Prüfung durchführt. 1 steht für gesund und 0 für ungesund.

Gültige Statistiken: Minimum, Durchschnitt und Maximum

Einheiten: keine

SSLHandshakeZeit

Die Durchschnittszeit in Millisekunden, die die Route 53-Zustandsprüfungen benötigten, um den SSL-Handshake abzuschließen. Sie können `SSLHandshakeTime` für eine Zustandsprüfung für die gesamten Regionen oder für eine ausgewählte geografische Region angezeigt bekommen.

Gültige Statistiken: Durchschnitt (empfohlen), Minimum, Maximum

Einheiten: Millisekunden

TimeToFirstByte

Die Durchschnittszeit in Millisekunden, bis die Route 53-Zustandsprüfungen die ersten Byte von einer Antwort auf eine HTTP- oder HTTPS-Anforderung erhalten haben. Sie können

`TimeToFirstByte` für eine Zustandsprüfung für die gesamten Regionen oder für eine ausgewählte geografische Region angezeigt bekommen.

Gültige Statistiken: Durchschnitt (empfohlen), Minimum, Maximum

Einheiten: Millisekunden

Dimensionen für Route 53-Metriken für Zustandsprüfungen

Route 53-Metriken für Zustandsprüfungen verwenden den Namespace `AWS/Route53` und stellen Metriken für `HealthCheckId` bereit. Wenn Sie Metriken abrufen, müssen Sie die Dimension `HealthCheckId` angeben.

Für `ConnectionTime`, `SSLHandshakeTime` und `TimeToFirstByte` können Sie optional `Region` hinzufügen. Wenn Sie den Wert weglassen`Region`, werden Kennzahlen für alle Regionen CloudWatch zurückgegeben. Wenn Sie angeben`Region`, werden nur Kennzahlen für die angegebene Region CloudWatch zurückgegeben.

Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

Überwachung von Hosting-Zonen mit Amazon CloudWatch

Sie können Ihre öffentlich gehosteten Zonen überwachen, indem Sie Amazon verwenden CloudWatch , um Rohdaten zu sammeln und zu lesbaren Metriken fast in Echtzeit zu verarbeiten. Metriken sind verfügbar, kurz nachdem Route 53 die DNS-Abfragen empfangen hat, auf denen die Metriken basieren. CloudWatch Metrikdaten für von Route 53 gehostete Zonen haben eine Granularität von einer Minute.

Weitere Informationen finden Sie in der folgenden Dokumentation

- Eine Übersicht und Informationen zum Anzeigen von Metriken in der CloudWatch Amazon-Konsole und zum Abrufen von Metriken mithilfe von AWS Command Line Interface (AWS CLI) finden Sie unter Anzeigen von DNS-Abfragemetriken für eine öffentliche gehostete Zone
- Informationen zur Aufbewahrungsfrist für Metriken finden Sie GetMetricStatisticsin der Amazon CloudWatch API-Referenz.
- Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

- Weitere Informationen zu CloudWatch Metriken finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Themen

CloudWatch Metriken für öffentlich gehostete Route 53-Zonen

Der `AWS/Route53`-Namespace enthält die folgenden Metriken für gehostete Route-53-Zonen:

DNSQueries

In einer gehosteten Zone die Anzahl der DNS-Abfragen, die Route 53 in einem angegebenen Zeitraum beantwortet.

Gültige Statistiken: Summe, SampleCount

Einheiten: Anzahl

Region: Route 53 ist ein globaler Service. Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben.

DNSSECInternalFehlschlag

Der Wert ist 1, wenn ein Objekt in der gehosteten Zonein INTERNAL_FAILUREZustand. Andernfalls lautet der Wert 0.

Gültige Statistiken: Summe

Einheiten: Anzahl

Volumen: 1 pro 4 Stunden und gehosteter Zone

Region: Route 53 ist ein globaler Service. Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben.

DNSSECKeySigningKeysNeedingAction

Anzahl der Schlüssel zur Schlüsselsignatur (KSKs), die den Status ACTION_NEEDED haben (aufgrund eines KMS-Fehlers).

Gültige Statistiken: Summe, SampleCount

Einheiten: Anzahl

Volumen: 1 pro 4 Stunden und gehosteter Zone

Region: Route 53 ist ein globaler Service. Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben.

DNSSECKeySigningKeyMaxNeedingActionAge

Die Zeit ist verstrichen, seit der Schlüsselsignierschlüssel (KSK) auf den Status ACTION_NEEDED gesetzt wurde.

Gültige Statistiken: Maximum

Einheiten: Sekunden

Volumen: 1 pro 4 Stunden und gehosteter Zone

Region: Route 53 ist ein globaler Service. Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben.

DNSSECKeySigningKeyAge

Die Zeit, die seit der Erstellung des Schlüsselsignierschlüssels (KSK) verstrichen ist (nicht seit der Aktivierung).

Gültige Statistiken: Maximum

Einheiten: Sekunden

Volumen: 1 pro 4 Stunden und gehosteter Zone

Region: Route 53 ist ein globaler Service. Um Metriken für gehostete Zonen abzurufen, müssen Sie als Region USA Ost (Nord-Virginia) angeben.

CloudWatch Dimension für Metriken der öffentlich gehosteten Zone von Route 53

Route 53-Metriken für gehostete Zonen verwenden den `AWS/Route53`-Namespace und stellen Metriken für `HostedZoneId` bereit. Um die Anzahl der DNS-Abfragen zu erhalten, müssen Sie die ID der gehosteten Zone in der Dimension `HostedZoneId` angeben.

Überwachung von Route 53 VPC Resolver-Endpunkten mit Amazon CloudWatch

Sie können Amazon verwenden CloudWatch , um die Anzahl der DNS-Abfragen zu überwachen, die von Route 53 VPC Resolver-Endpunkten weitergeleitet werden. Amazon CloudWatch sammelt und verarbeitet Rohdaten zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Ressourcen ausgeführt werden. Standardmäßig werden Metrikdaten für Resolver-Endpunkte automatisch in Intervallen von fünf Minuten CloudWatch gesendet. Das Fünf-Minuten-Intervall ist auch das kleinste Intervall, in dem die Metrikdaten gesendet werden können.

Weitere Informationen zu VPC Resolver finden Sie unter. Was ist Route 53 VPC Resolver? Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Metriken und Dimensionen für Route 53 VPC Resolver

Wenn Sie VPC Resolver so konfigurieren, dass DNS-Abfragen an Ihr Netzwerk weitergeleitet werden oder umgekehrt, beginnt VPC Resolver, alle fünf Minuten Metriken und Dimensionen zu senden, CloudWatch was ungefähr der Anzahl der weitergeleiteten Abfragen entspricht. Sie können die folgenden Verfahren verwenden, um die Metriken in der CloudWatch Konsole oder mithilfe von () anzuzeigen. AWS Command Line Interface AWS CLI

So zeigen Sie VPC-Resolver-Metriken mit der Konsole an CloudWatch

1. Öffnen Sie die CloudWatch Konsole unter. https://console.aws.amazon.com/cloudwatch/
2. Wählen Sie in der Navigationsleiste die Region, in der Sie den Endpunkt erstellt haben.
3. Wählen Sie im Navigationsbereich Metriken aus.
4. Wählen Sie auf der Registerkarte All metrics (Alle Metriken) die Option Route 53 Resolver.
5. Wählen Sie By Endpoint (Nach Endpunkt), um die Anzahl der Abfragen für einen bestimmten Endpunkt anzuzeigen. Wählen Sie dann die Endpunkte aus, für die Sie die Anzahl der Abfragen anzeigen möchten.

   Wählen Sie Across All Endpoints, um die Anzahl der Abfragen für alle eingehenden Endpunkte oder für alle ausgehenden Endpunkte anzuzeigen, die vom aktuellen Konto erstellt wurden.

AWS Wählen Sie dann InboundQueryVolumeoder, um die gewünschten Zählungen OutboundQueryVolumeanzuzeigen.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

- Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Themen

CloudWatch Grundlegende Metriken für Route 53 VPC Resolver

`AWS/Route53Resolver`Der Namespace enthält kostenlos grundlegende Metriken für Route 53 53-VPC-Resolver-Endpunkte und für IP-Adressen.

Themen

Metriken für Route 53 VPC Resolver-Endpunkte

Der `AWS/Route53Resolver` Namespace umfasst die folgenden Metriken für Route 53 VPC Resolver-Endpunkte.

EndpointHealthyENICount

Die Anzahl der Elastic Network-Schnittstellen im `OPERATIONAL`-Status. Die Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt (spezifiziert von `EndpointId`) sind ordnungsgemäß konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und Resolver weitergeben.

Gültige Statistiken: Minimum, Maximum, Durchschnitt

Einheiten: Anzahl

EndpointUnhealthyENICount

Die Anzahl der Elastic Network-Schnittstellen im `AUTO_RECOVERING`-Status.

Dies bedeutet, dass der Resolver versucht, eine oder mehrere der Amazon VPC Netzwerkschnittstellen wiederherzustellen, die dem Endpunkt zugeordnet sind (angegeben durch `EndpointId`). Während des Wiederherstellungsprozesses funktioniert der Endpunkt mit begrenzter Kapazität und kann keine DNS-Abfragen verarbeiten, bis er vollständig wiederhergestellt ist.

Gültige Statistiken: Minimum, Maximum, Durchschnitt

Einheiten: Anzahl

InboundQueryVolume

Für eingehende Endpunkte die Anzahl der DNS-Abfragen, die von Ihrem Netzwerk VPCs über den von angegebenen Endpunkt an Sie weitergeleitet wurden. `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryVolume

Bei ausgehenden Endpunkten die Anzahl der DNS-Anfragen, die von Ihrem an Ihr Netzwerk über VPCs den von angegebenen Endpunkt weitergeleitet wurden. `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryAggregateVolume

Für ausgehende Endpunkte die Gesamtzahl der DNS-Anfragen, die von Amazon VPCs an Ihr Netzwerk weitergeleitet wurden, einschließlich der folgenden:

- Die Anzahl der DNS-Anfragen, die von Ihrem VPCs an Ihr Netzwerk über den von angegebenen Endpunkt weitergeleitet wurden. `EndpointId`
- Wenn das aktuelle Konto die Resolver-Regeln mit anderen Konten teilt, werden Abfragen von VPCs diesem Konto von anderen Konten erstellt, die über den von `EndpointId` angegebenen Endpunkt an Ihr Netzwerk weitergeleitet werden.

Gültige Statistiken: Summe

Einheiten: Anzahl

ResolverEndpointCapacityStatus

Der Kapazitätsstatus des Resolver-Endpunkts. Die Metrik gibt den aktuellen Kapazitätsauslastungsstatus an, wobei: 0 = OK (normale Betriebskapazität), 1 = Warnung (mindestens eine Elastic Network-Schnittstelle überschreitet die Kapazitätsauslastung von 50%) und 2 = Kritisch (mindestens eine elastic network interface überschreitet die Kapazitätsauslastung von 75%).

Der Kapazitätsstatus wird durch mehrere Faktoren bestimmt, darunter Abfragevolumen, Abfragelatenz, DNS-Protokolle, DNS-Paketgröße und Verbindungsverfolgungsstatus.

Gültige Statistiken: Maximum

Einheiten: keine

Bewährte Methoden für das Kapazitätsmanagement von VPC Resolver Endpoints

Um Kapazitätsprobleme zu beheben, empfehlen wir generell, die Anzahl der Elastic Network-Schnittstellen für Ihren Resolver-Endpunkt zu erhöhen. Es gibt jedoch wichtige Überlegungen zu bestimmten Endpunkttypen:

Bei eingehenden Endpunkten hängt der Lastenausgleich des Datenverkehrs vom Kunden ab. Daher können Kapazitätswarnungen oder kritische Warnmeldungen auf einen „Hotspot“ hinweisen, an dem eine Untergruppe von Elastic Network-Schnittstellen überproportional genutzt wird.

- Um potenzielle Probleme mit dem Lastenausgleich zu identifizieren, sollten Sie die InboundQueryVolumeMetriken für jede elastic network interface einzeln untersuchen.

Bei ausgehenden Endpunkten wird der Datenverkehr automatisch über elastische Netzwerkschnittstellen verteilt. Kapazitätsprobleme können auf Probleme mit dem Ziel-Name-Server zurückzuführen sein oder darauf, dass Timeout-Abfragen mit hoher Latenz die Resolver-Netzwerkschnittstellen überfordern.

- In diesen Fällen ist es möglicherweise nicht effektiv, einfach die Elastic Network-Schnittstellen zu erhöhen, und wir empfehlen, den Ziel-Name-Server zu reparieren.

Metriken für Route 53 VPC Resolver-IP-Adressen

Der `AWS/Route53Resolver`-Namespace umfasst die folgenden Metriken für jede IP-Adresse, die einem Resolver-Eingangs- oder -Ausgangsendpunkt zugeordnet ist. (Wenn Sie einen Endpunkt angeben, erstellt VPC Resolver eine Amazon VPC elastic network interface.)

InboundQueryVolume

Für jede IP-Adresse für Ihre eingehenden Endpunkte die Anzahl der DNS-Abfragen, die von Ihrem Netzwerk an die angegebene IP-Adresse weitergeleitet werden. Jede IP-Adresse wird durch die IP-Adress-ID identifiziert. Sie können diesen Wert über die Route 53-Konsole abrufen. Auf der Seite für den betreffenden Endpunkt finden Sie im Abschnitt IP-Adressen die Spalte IP-Adress-ID. Sie können den Wert auch programmgesteuert mithilfe von abrufen. ListResolverEndpointIpAddresses

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryAggregateVolume

Für jede IP-Adresse Ihrer ausgehenden Endpunkte die Gesamtzahl der DNS-Anfragen, die von Amazon VPCs an Ihr Netzwerk weitergeleitet wurden, einschließlich der folgenden:

- Die Anzahl der DNS-Anfragen, die unter Verwendung der angegebenen IP-Adresse von Ihrem VPCs an Ihr Netzwerk weitergeleitet wurden.
- Wenn das aktuelle Konto die Resolver-Regeln mit anderen Konten teilt, werden Abfragen von VPCs diesem Konto von anderen Konten erstellt, die über die angegebene IP-Adresse an Ihr Netzwerk weitergeleitet werden.

Jede IP-Adresse wird durch die IP-Adress-ID identifiziert. Sie können diesen Wert über die Route 53-Konsole abrufen. Auf der Seite für den betreffenden Endpunkt finden Sie im Abschnitt IP-Adressen die Spalte IP-Adress-ID. Sie können den Wert auch programmgesteuert mithilfe von. ListResolverEndpointIpAddresses

Gültige Statistiken: Summe

Einheiten: Anzahl

CloudWatch Detaillierte Metriken für Route 53 VPC Resolver

Route 53 VPC Resolver bietet RNI Enhanced und Target Name Server Metrics als optionale Funktionen für Endgeräte. Diese Metriken werden in Intervallen von 1 Minute gesendet CloudWatch .

> **Note**
>
> - Detaillierte Metriken sind standardmäßig nicht aktiviert, können aber auf Endpunktebene aktiviert werden. Diese Metriken können beim Erstellen oder Aktualisieren von Endpunkten mithilfe der Flags und programmgesteuert aktiviert werden. RniEnhancedMetricsEnabled TargetNameServerMetricsEnabled Weitere Informationen erhalten Sie unter CreateResolverEndpoint und UpdateResolverEndpoint.
> - Für die Nutzung der detaillierten Metriken für den Route 53 Resolver-Endpunkt fallen CloudWatch Standardpreise und Gebühren an. Weitere Informationen finden Sie unter CloudWatch Amazon-Preise.

Themen

Verbesserte RNI-Metriken

Route 53 Resolver veröffentlicht erweiterte RNI-Metriken an Amazon CloudWatch zur Überwachung der Leistung und des Zustands von Resolver-Endpunkten und Resolver-IP-Adressen. Der `AWS/Route53Resolver` Namespace umfasst die folgenden erweiterten RNI-Metriken für eingehende und ausgehende Route 53 Resolver-Endpunkte in der Dimension: `EndpointId` `RniId`

P90 ResponseTime

Das 90. Perzentil der Antwortlatenz von DNS-Anfragen, die von der Resolver-IP (`RniId`) empfangen wurden, die dem Resolver-Endpunkt () zugeordnet ist `EndpointId`

Gültige Statistiken: Maximum

Einheiten: Mikrosekunden

ServFailQueries

Anzahl der SERVFAIL-Antworten für DNS-Abfragen, die an die dem Resolver-Endpunkt () zugeordnete Resolver-IP () `RniId` gesendet wurden `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

NxDomainQueries

Anzahl der NXDOMAIN-Antworten für DNS-Abfragen, die an die dem Resolver-Endpunkt (`RniId`) zugeordnete Resolver-IP () gesendet wurden `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

RefusedQueries

Anzahl der REFUSED-Antworten für DNS-Anfragen, die an die dem Resolver-Endpunkt (`RniId`) zugeordnete Resolver-IP () gesendet wurden `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

FormErrorQueries

Anzahl der FORMERR-Antworten für DNS-Abfragen, die an die dem Resolver-Endpunkt (`RniId`) zugeordnete Resolver-IP () gesendet wurden `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

TimeoutQueries

Anzahl der Timeouts für DNS-Abfragen, die an die dem Resolver-Endpunkt (`RniId`) zugeordnete Resolver-IP () gesendet wurden `EndpointId`

Gültige Statistiken: Summe

Einheiten: Anzahl

Metriken für Ziel-Nameserver

Route 53 Resolver veröffentlicht Ziel-Nameserver-Metriken an Amazon CloudWatch , um die Leistung und Verfügbarkeit von Ziel-Nameservern zu überwachen, die Resolver-Endpunkten zugeordnet sind. Der `AWS/Route53Resolver` Namespace umfasst die folgenden detaillierten Metriken für ausgehende Route 53-Resolver-Endpunkte in den Dimensionen: `EndpointID` `TargetNameServerIP`

P90 ResponseTime

Die 90. Perzentil-Antwortlatenz der Ziel-Name-Server-IP (`TargetNameServerIP`) für DNS-Abfragen, die über den Resolver-Endpunkt () gesendet werden `EndpointID`

Gültige Statistiken: Maximum

Einheiten: Mikrosekunden

RequestQueries

Anzahl der DNS-Abfragen, die über den Resolver-Endpunkt () an die Ziel-Name-Server-IP (`TargetNameServerIP`) gesendet wurden. `EndpointID`

Gültige Statistiken: Summe

Einheiten: Anzahl

TimeoutQueries

Anzahl der DNS-Abfragen, die über den Resolver-Endpunkt (`EndpointID`) gesendet wurden und bei denen das Timeout an der Ziel-Nameserver-IP () überschritten wurde. `TargetNameServerIP`

Gültige Statistiken: Summe

Einheiten: Anzahl

> **Note**
>
> In einigen Fällen können Lücken in den VPC Resolver-Metriken (ResolverEndpointCapacityStatus) und den erweiterten RNI-Metriken beobachtet werden. Diese Lücken können auftreten, wenn Ihre Netzwerkschnittstellen aufeinanderfolgend planmäßig gewartet oder aktualisiert werden. Nachdem wir eine Netzwerkschnittstelle wieder in Betrieb genommen haben, dauert es mindestens 1 Minute, bis unser Service Betriebsdaten

erfasst und diese Kennzahlen veröffentlicht. Diese Lücken deuten nicht darauf hin, dass Ihr VPC Resolver-Endpunkt ausgefallen ist. Wenn Sie einen CloudWatch Alarm für diese Metriken konfigurieren, empfehlen wir Folgendes:

- Stellen Sie den Alarm auf „Fehlende Daten als ignoriert behandeln“ ein, oder
- Konfigurieren Sie einen Evaluierungszeitraum von mehr als fünf Minuten für den Alarmschwellenwert.

Diese Einstellungen tragen dazu bei, Fehlalarme bei normalen Wartungsarbeiten zu reduzieren.

Dimensionen für Route 53 VPC Resolver-Metriken

Route 53 VPC Resolver-Metriken für eingehende und ausgehende Endpoints verwenden den `AWS/Route53Resolver` Namespace und stellen Metriken für die folgenden Dimensionen bereit:

- `EndpointId`: Wenn Sie einen Wert für die `EndpointId` Dimension angeben, wird die Anzahl der DNS-Abfragen für den angegebenen Endpunkt CloudWatch zurückgegeben. Wenn Sie keinen Wert angeben`EndpointId`, wird die Anzahl der DNS-Abfragen für alle Endpunkte CloudWatch zurückgegeben, die vom aktuellen AWS Konto erstellt wurden.
- `RniId`Dimension wird für `OutboundQueryAggregateVolume` `InboundQueryVolume` Metriken unterstützt.
- `EndpointId`, `RniId` Dimension wird für`P90ResponseTime`,,, `ServFailQueries` `NxDomainQueries` `RefusedQueries``FormErrorQueries`, und `TimeoutQueries` für die Resolver-IP-Adresse unterstützt, die dem Resolver-Endpunkt zugeordnet ist.
- `EndpointID`, `TargetNameServerIP` Dimension wird für `P90ResponseTime``RequestQueries`, und `TimeoutQueries` für den Ziel-Name-Server unterstützt, der dem Resolver-Endpunkt zugeordnet ist.

Überwachung von Resolver-DNS-Firewall-Regelgruppen mit Amazon CloudWatch

Sie können Amazon verwenden CloudWatch , um die Anzahl der DNS-Abfragen zu überwachen, die von Resolver DNS Firewall-Regelgruppen gefiltert werden. Amazon CloudWatch sammelt und

verarbeitet Rohdaten zu lesbaren Metriken, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Ressourcen ausgeführt werden. Standardmäßig werden Metrikdaten für DNS-Firewall-Regelgruppen automatisch CloudWatch in Intervallen von fünf Minuten gesendet.

Weitere Informationen zu DNS Firewall finden Sie unter Verwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr. Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Metriken und Dimensionen für die Resolver DNS Firewall

Wenn Sie einer VPC eine Resolver-DNS-Firewall-Regelgruppe zuordnen, um DNS-Abfragen zu filtern, beginnt die DNS-Firewall, alle 5 Minuten Metriken und Dimensionen an CloudWatch etwa die Abfragen zu senden, die sie filtert. Weitere Informationen zur Metrik und Dimension für DNS Firewall finden Sie unter CloudWatch Metriken für Resolver DNS Firewall.

Sie können die folgenden Verfahren verwenden, um die Metriken in der CloudWatch Konsole oder mithilfe von AWS Command Line Interface ()AWS CLI anzuzeigen.

So zeigen Sie DNS-Firewall-Metriken mit der CloudWatch Konsole an

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie auf der Navigationsleiste die Region aus, die Sie anzeigen möchten.
3. Wählen Sie im Navigationsbereich Metriken aus.
4. Wählen Sie auf der Registerkarte Alle Metriken die Option Route 53 VPC Resolver aus.
5. Wählen Sie eine Metrik aus, die Sie interessieren.

Um Metriken anzuzeigen, verwenden Sie AWS CLI

- Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Themen

- CloudWatch Metriken für Resolver DNS Firewall

CloudWatch Metriken für Resolver DNS Firewall

Der `AWS/Route53Resolver` Namespace enthält Metriken für Resolver DNS-Firewall-Regelgruppen.

Themen

Metriken für Resolver-DNS-Firewall-Regelgruppen

FirewallRuleGroupQueryVolume

Die Anzahl der DNS-Firewall-Abfragen, die einer Firewall-Regelgruppe entsprechen (angegeben durch`FirewallRuleGroupId`) enthalten.

Maße: `FirewallRuleGroupId`

Gültige Statistiken: Summe

Einheiten: Anzahl

Metriken für VPCs

VpcFirewallQueryVolume

Die Anzahl der DNS-Firewall-Abfragen von einer VPC (angegeben durch`VpcId`) enthalten.

Maße: `VpcId`

Gültige Statistiken: Summe

Einheiten: Anzahl

Metriken für Firewall-Regelgruppe und VPC Zuordnung

FirewallRuleGroupVpcQueryVolume

Die Anzahl der DNS-Firewall-Abfragen von einer VPC (angegeben durch`VpcId`), die mit einer Firewall-Regelgruppe übereinstimmen (angegeben durch`FirewallRuleGroupId`) enthalten.

Maße: `FirewallRuleGroupId, VpcId`

Gültige Statistiken: Summe

Einheiten: Anzahl

Metriken für eine Domainliste in einer Firewall-Regelgruppe

FirewallRuleQueryVolume

Die Anzahl der DNS-Firewall-Abfragen, die einer Firewall-Domainliste entsprechen (angegeben durch`FirewallDomainListId`) innerhalb einer Firewall-Regelgruppe (angegeben durch `FirewallRuleGroupId`) enthalten.

Maße: `FirewallRuleGroupId, FirewallDomainListId`

Gültige Statistiken: Summe

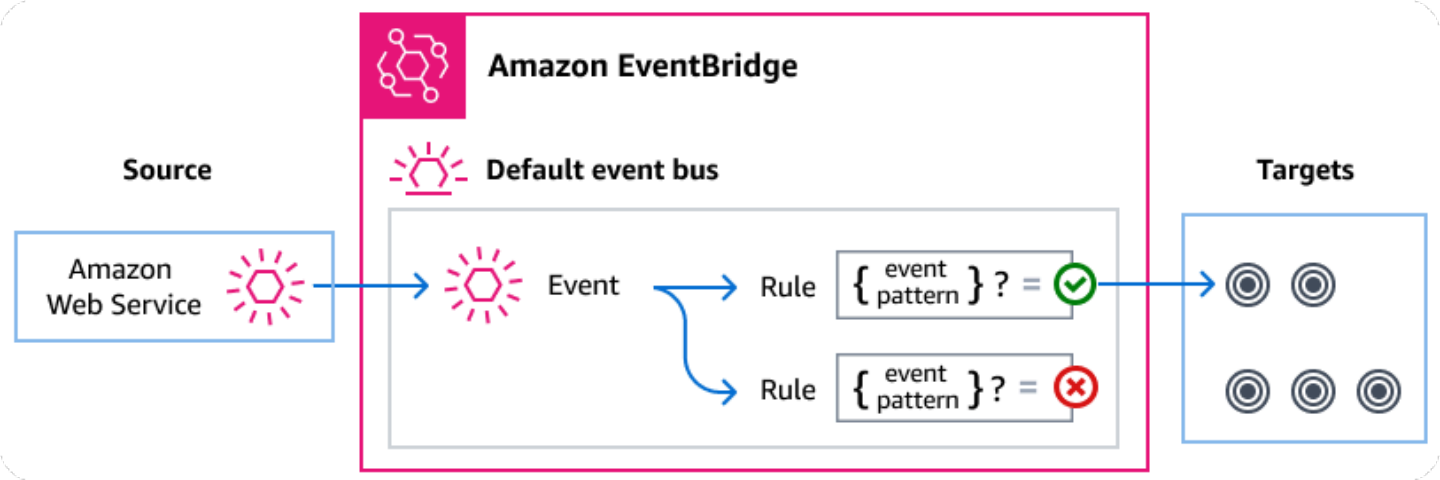
Einheiten: Anzahl

Verwaltung von Resolver-DNS-Firewall-Ereignissen mit Amazon EventBridge

Amazon EventBridge ist ein serverloser Dienst, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden, sodass Sie leichter skalierbare, ereignisgesteuerte Anwendungen erstellen können. Bei der ereignisgesteuerten Architektur werden lose gekoppelte Softwaresysteme entwickelt, die zusammenarbeiten, indem sie Ereignisse senden und darauf reagieren. Ereignisse stellen eine Veränderung in einer Ressource oder Umgebung dar.

Wie bei vielen AWS Diensten generiert die DNS-Firewall Ereignisse und sendet sie an den EventBridge Standard-Ereignisbus. (Der Standard-Event-Bus wird automatisch in jedem AWS Konto bereitgestellt.) Ein Event Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele weiterleitet. Die Regeln, die Sie für den Event Bus festlegen, werten die Ereignisse aus, sobald sie

eintreffen. Jede Regel prüft, ob ein Ereignis dem Ereignismuster der Regelentspricht. Wenn das Ereignis übereinstimmt, sendet der Event Bus das Ereignis an das/die angegebene(n) Ziel(e).



Themen

- Löst DNS-Firewall-Ereignisse auf
- Senden von Resolver-DNS-Firewall-Ereignissen mithilfe von Regeln EventBridge
- Amazon EventBridge Berechtigungen
- Zusätzliche EventBridge Ressourcen
- Detailreferenz zu Resolver-DNS-Firewall-Ereignissen

Löst DNS-Firewall-Ereignisse auf

VPC Resolver sendet DNS-Firewall-Ereignisse automatisch an den EventBridge Standardereignisbus. Sie können Regeln für den Event-Bus erstellen. Jede Regel umfasst ein Ereignismuster und ein oder mehrere Ziele. Ereignisse, die dem Ereignismuster einer Regel entsprechen, werden nach bestem Wissen und Gewissen an die angegebenen Ziele übermittelt. Ereignisse werden möglicherweise nicht in der richtigen Reihenfolge zugestellt.

Die folgenden Ereignisse werden von der DNS-Firewall generiert. Weitere Informationen finden Sie EventBridgeim Amazon EventBridge Benutzerhandbuch. .

Ereignisdetailtyp	Description
DNS-Firewall-Blockierung	Jede Blockaktion, die auf einer Domain ausgeführt wird.
DNS-Firewall-Warnung	Jede Warnungsaktion, die auf einer Domain ausgeführt wurde.

Senden von Resolver-DNS-Firewall-Ereignissen mithilfe von Regeln EventBridge

Damit der EventBridge Standardereignisbus DNS-Firewallereignisse an ein Ziel sendet, müssen Sie eine Regel erstellen, die ein Ereignismuster enthält, das den Daten in den gewünschten DNS-Firewallereignissen entspricht.

Das Erstellen einer Regel besteht aus den folgenden allgemeinen Schritten:

1. Erstellen eines Ereignismusters für die Regel, das Folgendes festlegt:
   - VPC Resolver ist die Quelle der Ereignisse, die von der Regel ausgewertet werden.
   - (Optional): Alle anderen Ereignisdaten, mit denen ein Abgleich durchgeführt werden kann.

   Weitere Informationen finden Sie unter ???.
2. (Optional): Erstellen eines Eingangstransformators, der die Daten aus dem Ereignis anpasst, EventBridge bevor die Informationen an das Ziel der Regel weitergegeben werden.

   Weitere Informationen finden Sie unter Eingabetransformation im EventBridge Benutzerhandbuch.
3. Geben Sie die Ziele an, an die Sie Ereignisse EventBridge senden möchten, die dem Ereignismuster entsprechen.

   Ziele können andere AWS Dienste, software-as-a-service (SaaS-) Anwendungen, API-Ziele oder andere benutzerdefinierte Endpunkte sein. Weitere Informationen finden Sie unter Ziele im Benutzerhandbuch für EventBridge .

Umfassende Anweisungen zum Erstellen von Event-Bus-Regeln finden Sie im EventBridge Benutzerhandbuch unter Erstellen von Regeln, die auf Ereignisse reagieren.

Ereignismuster für Resolver DNS Firewall-Ereignisse erstellen

Wenn die DNS-Firewall ein Ereignis an den Standardereignisbus übermittelt, bestimmt sie EventBridge anhand des für jede Regel definierten Ereignismusters, ob das Ereignis an die Ziele der Regel übermittelt werden soll. Ein Ereignismuster entspricht den Daten in den gewünschten DNS-Firewall-Ereignissen. Jedes Ereignismuster ist ein JSON-Objekt, das Folgendes enthält:

- Ein `source`-Attribut, das den Service identifiziert, der das Ereignis sendet. Für DNS-Firewall-Ereignisse lautet die Quelle`aws.route53resolver`.
- (Optional): Ein `detail-type`-Attribut, das ein Array der zuzuordnenden Ereignistypen enthält.

- (Optional): Ein `detail`-Attribut, das alle anderen Ereignisdaten für den Abgleich enthält.

Das folgende Ereignismuster entspricht beispielsweise sowohl den Warnungs- als auch den Blockierungsereignissen der DNS-Firewall:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Das folgende Ereignismuster entspricht zwar einer BLOCK-Aktion:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

Die DNS-Firewall sendet dasselbe Ereignis für dieselbe Domain nur einmal innerhalb eines 6-Stunden-Fensters. Beispiel:

1. Die Instanz i-123 hat zum Zeitpunkt T1 eine DNS-Abfrage exampledomain.com gesendet. Die DNS-Firewall sendet eine Warnung oder ein Blockierungsereignis, da dies das erste Ereignis ist.
2. Die Instanz i-123 hat zum Zeitpunkt DNSquery T1+30 Minuten eine Datei exampledomain.com gesendet. Die DNS-Firewall sendet keine Warnung und blockiert kein Ereignis, da es sich um ein wiederholtes Ereignis innerhalb des 6-Stunden-Fensters handelt.
3. Die Instanz i-123 hat zum Zeitpunkt T1+7 Stunden eine DNS-Abfrage exampledomain.com gesendet. Die DNS-Firewall sendet eine Warnung oder ein Blockierungsereignis, wenn dieses Ereignis außerhalb des 6-Stunden-Fensters auftritt.

Weitere Informationen zum Schreiben von Ereignismustern finden Sie unter Ereignismuster im EventBridge Benutzerhandbuch.

Testen von Ereignismustern für DNS-Firewall-Ereignisse in EventBridge

Sie können die EventBridge Sandbox verwenden, um schnell ein Ereignismuster zu definieren und zu testen, ohne den größeren Prozess der Erstellung oder Bearbeitung einer Regel abschließen zu müssen. Mithilfe der Sandbox können Sie ein Ereignismuster definieren und anhand eines

Beispielereignisses überprüfen, ob das Muster den gewünschten Ereignissen entspricht. EventBridge bieten Ihnen die Möglichkeit, anhand dieses Ereignismusters direkt in der Sandbox eine neue Regel zu erstellen.

Weitere Informationen finden Sie unter Testen eines Ereignismusters mithilfe der EventBridge Sandbox im EventBridge Benutzerhandbuch.

Eine EventBridge Regel und ein Ziel für die DNS-Firewall erstellen

Das folgende Verfahren zeigt Ihnen, wie Sie eine Regel erstellen, die das Senden von Ereignissen für alle Warnungs- und Blockierungsaktionen der DNS-Firewall ermöglicht EventBridge , und wie Sie eine AWS Lambda Funktion als Ziel für die Regel hinzufügen.

1. Verwenden Sie AWS CLI , um eine EventBridge Regel zu erstellen:

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. Hängen Sie eine Lambda-Funktion als Ziel für die Regel an:

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Führen Sie den folgenden AWS CLI Lambda-Befehl aus, um die zum Aufrufen des Ziels erforderlichen Berechtigungen hinzuzufügen:

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge Berechtigungen

Für die DNS-Firewall sind keine zusätzlichen Berechtigungen für die Übermittlung von Ereignissen erforderlich Amazon EventBridge.

Die von Ihnen angegebenen Ziele benötigen möglicherweise bestimmte Berechtigungen oder Konfigurationen. Weitere Informationen zur Verwendung bestimmter Dienste für Amazon EventBridge Ziele finden Sie im Amazon EventBridge Benutzerhandbuch unter Ziele.

Zusätzliche EventBridge Ressourcen

Weitere Informationen zur Verarbeitung und Verwaltung von Ereignissen finden Sie EventBridge in den folgenden Themen im Amazon EventBridge Benutzerhandbuch.

- Ausführliche Informationen zur Funktionsweise von Eventbussen finden Sie unter Amazon EventBridge Event-Bus.
- Informationen zur Veranstaltungsstruktur finden Sie unter Ereignisse.
- Informationen zur Erstellung von Ereignismustern, die beim EventBridge Abgleich von Ereignissen mit Regeln verwendet werden können, finden Sie unter Ereignismuster.
- Informationen zum Erstellen von Regeln, mit denen angegeben wird, welche Ereignisse EventBridge verarbeitet werden, finden Sie unter Regeln.
- Informationen zur Angabe, an welche Dienste oder andere Ziele EventBridge übereinstimmende Ereignisse senden, finden Sie unter Ziele.

Detailreferenz zu Resolver-DNS-Firewall-Ereignissen

Alle Ereignisse von AWS Diensten haben einen gemeinsamen Satz von Feldern, die Metadaten zu dem Ereignis enthalten, z. B. den AWS Dienst, der die Quelle des Ereignisses darstellt, den Zeitpunkt, zu dem das Ereignis generiert wurde, das Konto und die Region, in der das Ereignis stattgefunden hat, und andere. Definitionen dieser allgemeinen Felder finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

Darüber hinaus weist jedes Ereignis ein `detail`-Feld auf, das spezifische Daten für das betreffende Ereignis enthält. In der folgenden Referenz werden die Detailfelder für die verschiedenen DNS-Firewall-Ereignisse definiert.

Bei der EventBridge Auswahl und Verwaltung von DNS-Firewall-Ereignissen ist es hilfreich, Folgendes zu beachten:

- Das `source` Feld für alle Ereignisse der DNS-Firewall ist auf gesetzt`aws.route53resolver`.
- Das Feld `detail-type` gibt den Ereignistyp an.

  Zum Beispiel `DNS Firewall Block` oder `DNS Firewall Alert`.
- Das Feld `detail` enthält die Daten, die für das betreffende Ereignis spezifisch sind.

Informationen zur Erstellung von Ereignismustern, die es Regeln ermöglichen, DNS-Firewall-Ereignissen zu entsprechen, finden Sie unter Ereignismuster im Amazon EventBridge Benutzerhandbuch.

Weitere Informationen zu Ereignissen und deren EventBridge Verarbeitung finden Sie im Amazon EventBridge Benutzerhandbuch unter Amazon EventBridge Ereignisse.

Themen

Einzelheiten zum Ereignis der DNS-Firewall-Warnung

Im Folgenden finden Sie die Detailfelder für Details zum Warnstatus-Ereignis.

Die `detail-type` Felder `source` und sind enthalten, da sie spezifische Werte für Route 53-Ereignisse enthalten.

```
{...,
 "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
```

```
        "resolver-endpoint-details": {
        "id": "string"
      }
    }
]
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`DNS Firewall Alert`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für DNS-Firewall-Ereignisse ist dieser Wert`aws.route53resolver`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`account-id`

Die ID desjenigen AWS-Konto , der die VPC erstellt hat.

`last-observed-at`

Der Zeitstempel, zu dem die Alert/Block Abfrage in der VPC gestellt wurde.

`query-name`

Der Domainnamen (example.com) oder Subdomainname (www.example.com), der in der Abfrage angegeben wurde.

`query-type`

Entweder der DNS-Eintragstyp, der in der Anfrage angegeben wurde, oder ANY. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

`query-class`

Die ID der Abfrage.

`transport`

Das Protokoll, das zum Senden der DNS-Abfrage verwendet wird.

`firewall-rule-action`

Die Aktion, die von der Regel angegeben wurde, die dem Domainnamen in der Abfrage entspricht. Entweder `ALERT` oder `BLOCK`.

`firewall-rule-group-id`

Die ID des DNS-Firewall-Regelgruppe, die dem Domainnamen in der Abfrage entspricht. Weitere Informationen zu den Firewall-Regelgruppen finden Sie unter DNS-FirewallDNS-Firewall-Regelgruppen und -Regeln.

`firewall-domain-list-id`

Die Domainliste, die von der Regel verwendet wurde, die dem Domainnamen in der Abfrage entspricht.

`firewall-protection`

Erweiterter Schutz durch die DNS-Firewall: DGA, DICTIONARY_DGA oder DNS_TUNNELING. Weitere Informationen finden Resolver DNS Firewall Advanced Sie unter DNS-Firewall.

`resourcese`

Enthält Ressourcentypen und zusätzliche Informationen zu ihnen.

`resource-type`

Gibt den Ressourcentyp an, z. B. den Resolver-Endpunkt oder eine VPC-Instanz.

`resource-type``-detail`

Zusätzliche Details zur Ressource.

Example DNS-Firewall-Warnungsereignis

Im Folgenden finden Sie ein Beispiel für ein Alarmereignis.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
```

```
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DGA",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```


Einzelheiten zum DNS-Firewall-Blockereignis

Nachfolgend finden Sie die Detailfelder für*event name*.

Die `detail-type` Felder `source` und sind enthalten, da sie spezifische Werte für Route 53-Ereignisse enthalten.


```
{...,
```

```
 "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`DNS Firewall Alert`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für DNS-Firewall-Ereignisse ist dieser Wert`aws.route53resolver`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`account-id`

Die ID desjenigen AWS-Konto , der die VPC erstellt hat.

`last-observed-at`

Der Zeitstempel, zu dem die Alert/Block Abfrage in der VPC gestellt wurde.

`query-name`

Der Domainnamen (example.com) oder Subdomainname (www.example.com), der in der Abfrage angegeben wurde.

`query-type`

Entweder der DNS-Eintragstyp, der in der Anfrage angegeben wurde, oder ANY. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

`query-class`

Die ID der Abfrage.

`transport`

Das Protokoll, das zum Senden der DNS-Abfrage verwendet wird.

`firewall-rule-action`

Die Aktion, die von der Regel angegeben wurde, die dem Domainnamen in der Abfrage entspricht. Entweder `ALERT` oder `BLOCK`.

`firewall-rule-group-id`

Die ID des DNS-Firewall-Regelgruppe, die dem Domainnamen in der Abfrage entspricht. Weitere Informationen zu den Firewall-Regelgruppen finden Sie unter DNS-FirewallDNS-Firewall-Regelgruppen und -Regeln.

`firewall-domain-list-id`

Die Domainliste, die von der Regel verwendet wurde, die dem Domainnamen in der Abfrage entspricht.

`firewall-protection`

Erweiterter Schutz durch die DNS-Firewall: DGA, DICTIONARY_DGA oder DNS_TUNNELING. Weitere Informationen finden Resolver DNS Firewall Advanced Sie unter DNS-Firewall.

`resourcese`

Enthält Ressourcentypen und zusätzliche Informationen zu ihnen.

`resource-type`

Gibt den Ressourcentyp an, z. B. den Resolver-Endpunkt oder eine VPC-Instanz.

`resource-type``-detail`

Zusätzliche Details zur Ressource.

Example Beispielereignis

Im Folgenden finden Sie ein Beispiel für ein Blockereignis.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DNS_TUNNELING",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
```

```
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```

Protokollieren von Amazon Route 53-API-Aufrufen mit AWS CloudTrail

Route 53 ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Route 53 ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Route 53 als Ereignisse, einschließlich Aufrufe von der Route 53-Konsole und von Codeaufrufen an Route APIs 53. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Route 53. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Route 53 gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Themen

- Route 53-Informationen in CloudTrail
- Anzeigen von Route 53-Ereignissen mit dem Ereignisverlauf
- Grundlagen zu Route 53 log Protokolldateieinträgen

Route 53-Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn auf Route 53 Aktivitäten auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Route 53, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Route 53-Aktionen werden von der Amazon Route 53 API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Aufrufe der `RegisterDomain` Aktionen, `CreateHostedZoneCreateHealthCheck`, und generieren beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anforderung mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Anzeigen von Route 53-Ereignissen mit dem Ereignisverlauf

CloudTrail ermöglicht es Ihnen, aktuelle Ereignisse im Ereignisverlauf anzuzeigen. Um Ereignisse für Route 53-API-Anforderungen anzuzeigen, müssen Sie die Option USA Ost (Nord-Virginia) in der Regionsauswahl oben in der Konsole auswählen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Grundlagen zu Route 53 log Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das `eventName`-Element kennzeichnet die erfolgte Aktion. (In CloudTrail Protokollen ist der erste Buchstabe für Domainregistrierungsaktionen ein Kleinbuchstabe, obwohl er in den Namen der Aktionen in Großbuchstaben geschrieben ist. `UpdateDomainContact`Erscheint beispielsweise wie `updateDomainContact` in den Protokollen). CloudTrail unterstützt alle Route 53-API-Aktionen. Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die folgenden Aktionen demonstriert:

- Listet die Hosting-Zonen auf, die einem AWS Konto zugeordnet sind
- Erstellen einer Zustandsprüfung
- Erstellen von zwei Datensätzen
- Löschen einer gehosteten Zone
- Aktualisieren der Informationen für eine registrierte Domain
- Erstellen Sie einen ausgehenden Route 53 VPC Resolver-Endpunkt


```
{
    "Records": [
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
            "eventName": "ListHostedZones",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2015-01-16T00:41:48Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": null,
            "responseElements": null,
            "sourceIPAddress": "192.0.2.92",
```

```
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
            "eventName": "CreateHealthCheck",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:57Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "callerReference": "2014-05-06 64832",
                "healthCheckConfig": {
                    "iPAddress": "192.0.2.249",
                    "port": 80,
                    "type": "TCP"
                }
            },
            "responseElements": {
                "healthCheck": {
                    "callerReference": "2014-05-06 64847",
                    "healthCheckConfig": {
                        "failureThreshold": 3,
                        "iPAddress": "192.0.2.249",
                        "port": 80,
                        "requestInterval": 30,
                        "type": "TCP"
                    },
                    "healthCheckVersion": 1,
                    "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
                },
                "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
```

```
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "additionalEventData": {
                "Note": "Do not use to reconstruct hosted zone"
            },
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
            "eventName": "ChangeResourceRecordSets",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:43Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "changeBatch": {
                    "changes": [
                        {
                            "action": "CREATE",
                            "resourceRecordSet": {
                                "name": "prod.example.com.",
                                "resourceRecords": [
                                    {
                                        "value": "192.0.1.1"
                                    },
                                    {
                                        "value": "192.0.1.2"
                                    },
                                    {
                                        "value": "192.0.1.3"
                                    },
                                    {
```

```
                                "value": "192.0.1.4"
                            }
                        ],
                        "tTL": 300,
                        "type": "A"
                    }
                },
                {
                    "action": "CREATE",
                    "resourceRecordSet": {
                        "name": "test.example.com.",
                        "resourceRecords": [
                            {
                                "value": "192.0.1.1"
                            },
                            {
                                "value": "192.0.1.2"
                            },
                            {
                                "value": "192.0.1.3"
                            },
                            {
                                "value": "192.0.1.4"
                            }
                        ],
                        "tTL": 300,
                        "type": "A"
                    }
                }
            ],
            "comment": "Adding subdomains"
        },
        "hostedZoneId": "Z1PA6795UKMFR9"
    },
    "responseElements": {
        "changeInfo": {
            "comment": "Adding subdomains",
            "id": "/change/C156SRE0X2ZB10",
            "status": "PENDING",
            "submittedAt": "Jan 16, 2018 12:41:43 AM"
        }
    },
    "sourceIPAddress": "192.0.2.92",
    "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
```

```
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "0cb87544-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": "444455556666"
        },
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
                        "creationDate": "2018-11-01T14:33:09Z"
                    },
                    "sessionIssuer": {
                        "type": "Role",
                        "principalId": "AROAIUZEZLWWZOEXAMPLE",
                        "arn": "arn:aws:iam::123456789012:role/Admin",
                        "accountId": "123456789012",
                        "userName": "Admin"
                    }
                }
            },
            "eventTime": "2018-11-01T14:37:19Z",
            "eventSource": "route53resolver.amazonaws.com",
            "eventName": "CreateResolverEndpoint",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.176",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
 Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "creatorRequestId": "123456789012",
                "name": "OutboundEndpointDemo",
                "securityGroupIds": [
                    "sg-05618b249example"
                ],
                "direction": "OUTBOUND",
                "ipAddresses": [
                    {
                        "subnetId": "subnet-01cb0c4676example"
                    },
                    {
                        "subnetId": "subnet-0534819b32example"
                    }
                ],
                "tags": []
            },
            "responseElements": {
                "resolverEndpoint": {
                    "id": "rslvr-out-1f4031f1f5example",
                    "creatorRequestId": "123456789012",
                    "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
```

```
                    "name": "OutboundEndpointDemo",
                    "securityGroupIds": [
                        "sg-05618b249example"
                    ],
                    "direction": "OUTBOUND",
                    "ipAddressCount": 2,
                    "hostVPCId": "vpc-0de29124example",
                    "status": "CREATING",
                    "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
 Creating the Resolver Endpoint",
                    "creationTime": "2018-11-01T14:37:19.045Z",
                    "modificationTime": "2018-11-01T14:37:19.045Z"
                }
            },
            "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",
            "eventID": "cb05b4f9-9411-4507-813b-33cb0example",
            "eventType": "AwsApiCall",
            "recipientAccountId": "123456789012"
        }
    ]
}
```

Fehlerbehebung bei Amazon Route 53

Auf dieser Seite werden die folgenden Themen zur Fehlerbehebung für Amazon Route 53 behandelt:

1. Domain nicht verfügbar:
   - Machen Sie sich mit häufigen Gründen vertraut, warum Ihre Domain im Internet möglicherweise nicht verfügbar ist, z. B. wenn die E-Mail-Adresse des Registranten nicht bestätigt wurde, Probleme mit der DNS-Dienstübertragung auftreten, falsche Nameservereinstellungen vorgenommen wurden oder gehostete Zonen gelöscht wurden.
2. Sperrung der Domain:
   - Erfahren Sie mehr über die Ursachen der Domain-Sperre (ClientHold Status) und darüber, wie Sie Ihre Domain entsperren können, einschließlich abgelaufener Domains, E-Mail-Änderungen nicht verifizierter Registranten und Probleme bei der Zahlungsabwicklung.
3. Fehlgeschlagener Domainvorgang:
   - Beheben Sie Fehler beim Domainbetrieb, einschließlich Problemen bei der Registrierung, Übertragung, Verlängerung und Kontaktaktualisierung, die durch ungültige Kontaktinformationen verursacht wurden.
4. Fehlgeschlagene Domainübertragung:
   - Entdecken Sie die häufigsten Gründe für eine fehlgeschlagene Domainübertragung auf Route 53, z. B. die Nichtautorisierung der Übertragung, ungültige Autorisierungscodes oder Probleme mit internationalisierten Domainnamen.
5. DNS-Einstellungen werden nicht wirksam:
   - Beheben Sie Situationen, in denen Ihre Änderungen an den DNS-Einstellungen noch nicht wirksam wurden, z. B. beim Zwischenspeichern von DNS-Resolvern, falschen Nameserver-Updates und mehreren Hosting-Zonen mit demselben Namen.
6. Fehler „Server nicht gefunden“:
   - Suchen Sie in Ihrem Browser nach Lösungen für Fehler „Server nicht gefunden“, z. B. für fehlende Datensätze, falsche Datensatzwerte oder nicht verfügbare Ressourcen.
7. Weiterleitung des Datenverkehrs an S3-Buckets:
   - Beheben Sie Probleme beim Versuch, Traffic an einen Amazon S3 S3-Bucket weiterzuleiten, der für das Hosting von Websites konfiguriert ist.
8. Probleme mit der Abrechnung:

- Machen Sie sich mit häufigen Abrechnungsszenarien vertraut, z. B. mit zweimaliger Abrechnung für dieselbe Hosting-Zone, mit mehreren Rechnungen für Domains und mit Problemen bei der Domainregistrierung, wenn Ihre Zone geschlossen oder dauerhaft geschlossen AWS-Konto ist.

Themen

Meine Domäne ist im Internet nicht verfügbar

Hier finden Sie die häufigsten Gründe dafür, warum Ihre Domäne im Internet nicht verfügbar ist.

Themen

Sie haben eine neue Domäne registriert, den Link in der Bestätigungs-E-Mail aber nicht angeklickt.

Wenn Sie eine neue Domäne registrieren, verlangt ICANN eine Bestätigung, dass die E-Mail-Adresse für den Registrierenden gültig ist. Um die Bestätigung zu erhalten, senden wir eine E-Mail mit einem Link. (Wenn Sie auf die erste E-Mail nicht reagieren, senden wir dieselbe E-Mail bis zu zwei weitere Male.) Sie haben je nach Top-Level-Domain zwischen 3 und 15 Tage Zeit, um auf den Link zu klicken. Nach dieser Zeit wird der Link funktionsunfähig.

Wenn Sie innerhalb der Frist nicht auf den Link in der E-Mail klicken, verlangt ICANN, dass wir die Domäne sperren. Weitere Informationen dazu, wie die Bestätigungs-E-Mail erneut an den Registrierenden gesendet wird, finden Sie unter Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails.

Sie haben eine Domainregistrierung an Amazon Route 53 übertragen, aber keinen DNS-Dienst.

Wenn Ihre vorherige Vergabestelle einen kostenlosen DNS-Dienst mit der Domänenregistrierung angeboten hat, hat die Vergabestelle diesen DNS-Dienst womöglich eingestellt, als Sie die Domänenregistrierung in Route 53 übertragen haben. Führen Sie die folgenden Schritte aus, um zu ermitteln, ob dies das Problem ist, und es gegebenenfalls dann auch zu lösen.

Vorgehensweise zum Wiederherstellen des DNS-Dienstes, wenn die vorherige Vergabestelle diesen nach Übertragung der Domänenregistrierung in Route 53 eingestellt hat

1. Wenden Sie sich an Ihre vorherige Vergabestelle und vergewissern Sie sich, dass sie den DNS-Dienst für Ihre Domäne eingestellt hat. Wenn dies der Fall ist, sind dies die drei schnellsten Möglichkeiten für die Wiederherstellung des DNS-Dienstes für die Domäne (von der wünschenswertesten zur am wenigsten wünschenswerten):

   - Wenn der vorherige Anbieter einen kostenpflichtigen DNS-Dienst bereitstellt, bitten Sie ihn um die Wiederherstellung des DNS-Dienstes mithilfe der alten DNS-Datensätze und der Namenserver für Ihre Domäne.
   - Wenn der vorherige Anbieter keinen kostenpflichtigen DNS-Dienst ohne Domänenregistrierung anbietet, fragen Sie ihn, ob Sie die Domänenregistrierung zurück zu ihm übertragen können. Bitten Sie ihn anschließend um die Wiederherstellung des DNS-Dienstes mithilfe der alten DNS-Datensätze und der Namenserver für Ihre Domäne.

- Wenn Sie die Domänenregistrierung zum vorherigen Anbieter zurückübertragen können, dieser aber Ihre DNS-Datensätze nicht mehr hat, fragen Sie ihn, ob Sie die Domänenregistrierung zurückübertragen und dieselbe Reihe von Namenservern erhalten können, die der Domäne auch vorher zugeordnet war. Wenn dies möglich ist, müssen Sie Ihre alten DNS-Datensätze selbst wiederherstellen. Sobald Sie dies tun, wird Ihre Domäne wieder sichtbar.

Wenn Ihre vorherige Vergabestelle Ihnen keine dieser Optionen bieten kann, fahren Sie mit Schritt 2 fort.

> **Important**
>
> Wenn Sie den DNS-Dienst nicht unter Verwendung der Namenserver wiederherstellen können, die Sie bei der Übertragung Ihrer Domäne in Route 53 angegeben haben, kann es nach Durchführung der restlichen Schritte in diesem Vorgang noch bis zu zwei Tage dauern, bis Ihre Domäne im Internet wieder sichtbar wird. DNS-Resolver speichern die Namen der Namenserver für eine Domäne in der Regel 24 bis 48 Stunden lang im Cache und es dauert so lange, bis alle DNS-Resolver die Namen der neuen Namenserver erhalten.

2. Wählen Sie einen neuen DNS-Dienst, wie z. B. Route 53.
3. Erstellen Sie mithilfe der Methode des neuen DNS-Dienstes eine gehostete Zone und Datensätze:

   a. Erstellen Sie eine gehostete Zone mit demselben Namen wie Ihre Domäne, beispielsweise example.com.

   b. Verwenden Sie die Zonendatei, die Sie von der vorherigen Vergabestelle erhalten haben, um Datensätze zu erstellen.

   Wenn Sie Route 53 als neuen DNS-Dienst wählen, können Sie Datensätze erstellen, indem Sie die Zonendatei importieren. Weitere Informationen finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.
4. Rufen Sie die Namenserver für die neue gehostete Zone ab. Wenn Sie Route 53 als DNS-Dienst wählen, informieren Sie sich unter Das Abrufen der Nameserver für eine öffentliche gehostete Zone.

5. Ändern Sie die Namenserver für Ihre Domäne: Stellen Sie die Namenserver ein, die Sie in Schritt 4 erhalten haben. Weitere Informationen finden Sie unter Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.

Sie haben die Domänenregistrierung übertragen und die falschen Namenserver in den Domäneneinstellungen angegeben.

Wenn Sie die Domainregistrierung an Amazon Route 53 übertragen, ist eine der Einstellungen, die Sie für die Domain angeben müssen, die Reihe von Namenservern, die auf DNS-Abfragen für die Domain antworten. Diese Namenserver stammen aus der gehosteten Zone, die denselben Namen wie die Domäne hat. Die gehostete Zone enthält Informationen darüber, wie Sie den Datenverkehr für die Domäne weiterleiten möchten, wie z. B. die IP-Adresse eines Webservers für www.example.com.

Möglicherweise haben Sie versehentlich die Namenserver für die falsche gehostete Zone angegeben. Das kann schnell passieren, wenn Sie mehr als eine gehostete Zone mit demselben Namen wie die Domäne haben. Gehen Sie wie folgt vor, um zu überprüfen, ob die Domäne die Namenserver für die richtige gehostete Zone verwendet, und die Namenserver für die Domäne gegebenenfalls zu aktualisieren.

> **Important**
>
> Wenn Sie bei der Übertragung der Domäne in Route 53 die falschen Namenserver-Datensätze angegeben haben, kann es nach Korrektur der Namenserver für die Domäne bis zu zwei Tage dauern, bis der DNS-Dienst vollständig wiederhergestellt ist. Der Grund dafür ist, dass die DNS-Resolver im Internet die Namenserver in der Regel nur einmal alle zwei Tage anfordern und die Antwort im Cache speichern.

Vorgehensweise zum Abrufen der Namenserver für Ihre gehostete Zone

1. Wenn Sie einen anderen DNS-Dienst für die Domäne verwenden, wenden Sie die vom DNS-Dienst bereitgestellte Methode zum Abrufen der Namenserver für die gehostete Zone an. Gehen Sie dann zum nächsten Schritt über.

   Wenn Sie Route 53 als DNS-Dienst für die Domain verwenden, melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.

2. Klicken Sie im Navigationsbereich auf Hosted Zones.
3. Wählen Sie auf der Seite Hosted Zones das Optionsfeld (nicht den Namen) für die gehostete Zone aus.

> **Important**
>
> Wenn Sie mehr als eine gehostete Zone mit demselben Namen haben, stellen Sie sicher, dass Sie die Namenserver für die richtige gehostete Zone abrufen.

4. Notieren Sie die vier Server, die im Bereich rechts als Name Servers aufgeführt werden.

Vorgehensweise zum Überprüfen, ob die Domäne die richtigen Namenserver verwendet

1. Wenn Sie einen anderen DNS-Dienst für die Domain verwenden, melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/

   Wenn Sie Route 53 verwenden, fahren Sie mit dem nächsten Schritt fort.
2. Klicken Sie im Navigationsbereich auf Registered Domains.
3. Wählen Sie den Namen der Domäne aus, für die Sie die Einstellungen bearbeiten möchten.
4. Klicken Sie auf Add or Edit Name Servers.
5. Vergleichen Sie die Liste der Namenserver, die Sie im vorherigen Vorgang erhalten haben, mit den Namenservern, die im Dialogfenster Edit Name Servers for Domänenname aufgelistet sind.
6. Wenn die hier aufgelisteten Namenserver nicht mit den Namenservern aus dem vorherigen Vorgang übereinstimmen, ändern Sie die Namenserver hier und klicken Sie auf Aktualisieren.

Sie haben den DNS-Dienst zuerst übertragen, aber nicht lange genug gewartet, um die Domänenregistrierung zu übertragen.

Als Sie den DNS-Dienst an Amazon Route 53 oder einen anderen DNS-Dienst übertragen haben, haben Sie die Konfiguration für Ihre Domain bei der Domainvergabestelle aktualisiert, sodass die Namenserver für den neuen DNS-Dienst verwendet werden.

DNS-Resolver, die auf Anfragen für Ihre Domäne antworten, speichern die Namen von Namenservern in der Regel 24 bis 48 Stunden lang im Cache. Wenn Sie den DNS-Dienst für eine Domäne ändern und die Namenserver eines DNS-Dienst mit den Namenservern für einen anderen

DNS-Dienst ersetzen, kann es bis zu 48 Stunden dauern, bis DNS-Resolver die neuen Namenserver und dementsprechend auch den neuen DNS-Dienst verwenden.

Im Nachfolgenden wird beschrieben, wie die Übertragung des DNS-Dienst und die zu frühe Übertragung Ihrer Domäne zur Nichtverfügbarkeit Ihrer Domäne im Internet führen kann:

1. Sie haben den DNS-Dienst für Ihre Domäne übertragen.
2. Sie haben Ihre Domäne in Route 53 übertragen, bevor DNS-Resolver mit der Verwendung der Namenserver für Ihren neuen DNS-Dienst begonnen haben.
3. Ihr vorheriger Anbieter hat den DNS-Dienst für Ihre Domäne eingestellt, sobald die Domäne in Route 53 übertragen wurde.
4. DNS-Resolver leiten Abfragen immer noch an Ihren alten DNS-Dienst weiter, es gibt aber keine Datensätze mit Anweisungen zur Weiterleitung Ihres Datenverkehrs mehr.

Wenn die im Cache gespeicherten Daten für die Namenserver für den alten DNS-Dienst ablaufen, wird Ihr neuer DNS-Dienst verwendet. Leider gibt es keine Möglichkeit, diesen Prozess zu beschleunigen.

Sie haben die gehostete Zone gelöscht, die Route 53 zum Weiterleiten des Internetdatenverkehrs an die Domäne verwendet

Wenn Route 53 der DNS-Dienst für Ihre Domäne ist und Sie die gehostete Zone löschen, die zum Weiterleiten des Internetdatenverkehrs an die Domäne verwendet wird, ist die Domäne im Internet nicht mehr erreichbar. Dies gilt unabhängig davon, ob die Domäne mit Route 53 registriert ist.

> **Important**
>
> Das Wiederherstellen des Internetservice für die Domäne kann bis zu 48 Stunden dauern.

So stellen Sie einen Internetservice her, wenn Sie eine gehostete Zone löschen, die Route 53 zum Weiterleiten des Internetdatenverkehrs an die Domäne verwendet

1. Erstellen Sie eine weitere gehostete Zone, die den gleichen Namen wie die Domäne hat. Weitere Informationen finden Sie unter Erstellen einer öffentlichen gehosteten Zone.
2. Erstellen Sie die Datensätze neu, die sich in der von Ihnen gelöschten gehosteten Zone befanden. Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

3. Rufen Sie die Namen der Namensserver ab, die der neuen gehosteten Zone von Route 53 zugewiesen wurden. Weitere Informationen finden Sie unter Das Abrufen der Nameserver für eine öffentliche gehostete Zone.
4. Aktualisieren Sie die Domänenregistrierung zur Verwendung der in Schritt 3 abgerufenen Namensserver:

   - Wenn die Domäne mit Route 53 registriert wurde, lesen Sie Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne.
   - Wenn die Domäne bei einer anderen Domänenvergabestelle registriert ist, verwenden Sie die Methode der Vergabestelle, um die Domänenregistrierung zur Verwendung der neuen Namensserver zu aktualisieren.
5. Warten Sie, bis die TTL die Namensserver an die rekursiven Resolver übergeben hat, die die Namen der Namensserver für die gelöschte gehostete Zone gespeichert haben. Nachdem die TTL abgelaufen ist oder wenn ein Browser oder eine Anwendung eine DNS-Abfrage für die Domäne oder eine ihrer Subdomänen sendet, leitet ein rekursiver Resolver die Abfrage an die Route-53-Namensserver für die neue gehostete Zone weiter. Weitere Informationen finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

   Die TTL für Namensserver kann bis zu 48 Stunden betragen, abhängig von der TLD der Domäne.

Ihre Domäne wurde gesperrt.

Ihre Domäne ist womöglich nicht im Internet verfügbar, weil wir sie sperren mussten. Weitere Informationen finden Sie unter Meine Domain ist gesperrt (Status ist ClientHold).

Meine Domain ist gesperrt (Status ist ClientHold)

Wenn Amazon Route 53 Ihre Domain sperrt, ist diese im Internet nicht mehr verfügbar. Sie können eine der folgenden Methoden verwenden, um zu ermitteln, ob eine Domäne gesperrt wurde:

- Suchen Sie auf der Seite Registered domains (Registrierte Domänen) der Route-53-Konsole den Domänennamen in der Tabelle Alerts (Warnungen) unten auf der Seite. Wenn der Wert in der Spalte Status clientHold ist, wurde die Domäne gesperrt.
- Senden Sie eine WHOIS-Abfrage für die Domäne. Wenn der Wert für Domain Status clientHold ist, wurde die Domäne gesperrt. Der WHOIS-Befehl ist in vielen Betriebssystemen verfügbar und steht zudem als Webanwendung auf vielen Webseiten zur Verfügung.

Wenn wir eine Domäne sperren, senden wir in der Regel zudem eine E-Mail an die E-Mail-Adresse des Registrierenden für die Domäne. Wenn die Domäne jedoch aufgrund eines Gerichtsbeschlusses gesperrt wurde, verbietet es uns das Gericht vielleicht, den Registrierenden zu benachrichtigen.

Damit eine Domäne wieder im Internet verfügbar ist, muss die Sperrung aufgehoben werden. Dies sind die Gründe, warum eine Domäne gesperrt werden kann, und die Vorgehensweisen, um die Sperrung aufzuheben.

> **Note**
>
> Wenn Sie Hilfe bei der Aufhebung der Sperre Ihrer Domain benötigen, können Sie sich kostenlos an den AWS Support wenden. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

Themen

Sie haben eine neue Domäne registriert, den Link in der Bestätigungs-E-Mail aber nicht angeklickt.

Wenn Sie eine Domain bei AWS zum ersten Mal registrieren, verlangt ICANN, dass wir eine Bestätigung erhalten, dass die E-Mail-Adresse für den Registrantenkontakt gültig ist. Um die Bestätigung zu erhalten, senden wir eine E-Mail mit einem Link. Sie haben je nach Top-Level-Domain zwischen 3 und 15 Tage Zeit, um auf den Link zu klicken. Nach dieser Zeit wird der Link funktionsunfähig.

> **Note**
>
> Wenn Sie bereits eine oder mehrere Domänen in Amazon Route 53 registriert haben und dieselbe E-Mail-Adresse für den Registrierenden verwendet haben, senden wir keine Bestätigungs-E-Mail.

Wenn Sie innerhalb der Frist nicht auf den Link in der E-Mail klicken, verlangt ICANN, dass wir die Domäne sperren. Weitere Informationen dazu, wie die Bestätigungs-E-Mail erneut an den Registrierenden gesendet wird, finden Sie unter Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails. Wenn Sie bestätigen, dass die E-Mail-Adresse gültig ist, wird die Sperrung der Domäne automatisch aufgehoben.

Sie haben die automatische Verlängerung für die Domäne deaktiviert und die Domäne ist abgelaufen.

Wenn die automatische Verlängerung für eine Domäne aktiviert ist (der Standardwert für eine neue oder übertragene Domäne), wird die Registrierung für eine Domäne kurz vor dem Ablaufdatum automatisch verlängert. Wenn Sie die automatische Verlängerung deaktivieren, senden wir drei E-Mails an die E-Mail-Adresse des Registrierenden, um daran zu erinnern, dass die Domänenregistrierung bald abläuft. Wir senden die erste E-Mail 45 Tage vor Ablauf der Domäne.

Wenn Sie die automatische Verlängerung deaktivieren und den Registrierungszeitraum für die Domäne nicht manuell verlängern, wird die Domäne in der Regel am Ablaufdatum gesperrt. Beachten Sie, dass die Registrys für einige Domänen die Domäne sogar vor dem Ablaufdatum sperren.

Weitere Informationen zum Erneuern einer abgelaufenen Domäne finden Sie unter Verlängern der Registrierung für eine Domain.

Sie haben die E-Mail-Adresse für den Registranten-Kontakt geändert, aber nicht überprüft, ob die neue E-Mail-Adresse gültig ist

Wenn Sie die E-Mail-Adresse für den Registranten-Kontakt in eine Adresse ändern, die Sie zuvor nicht überprüft haben, verlangt ICANN von uns, eine Bestätigung anzufordern, dass die E-Mail-Adresse für den Registranten-Kontakt gültig ist. Um die Bestätigung zu erhalten, senden wir eine E-Mail mit einem Link. Sie haben je nach Top-Level-Domain zwischen 3 und 15 Tage Zeit, um auf den Link zu klicken. Nach dieser Zeit wird der Link funktionsunfähig.

Wenn Sie innerhalb der von der TLD-Registrierungsstelle gewährten Frist nicht auf den Link in der E-Mail klicken, verlangt ICANN, dass wir die Domäne sperren. Weitere Informationen dazu, wie die Bestätigungs-E-Mail erneut an den Registrierenden gesendet wird, finden Sie unter Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails. Wenn Sie bestätigen, dass die E-Mail-Adresse gültig ist, wird die Sperrung der Domäne automatisch aufgehoben.

Wir konnten Ihre Zahlung für die automatische Domänenverlängerung nicht verarbeiten und die Domäne ist abgelaufen.

Wenn die automatische Verlängerung für eine Domäne aktiviert ist, wir Ihre Zahlung aber nicht verarbeiten konnten (weil beispielsweise Ihre Kreditkarte abgelaufen ist), senden wir mehrere E-Mails an die E-Mail-Adresse des Registrierenden für die Domäne. Wenn wir keine Zahlung erhalten, wird die Domäne in der Regel am Ablaufdatum gesperrt. Beachten Sie, dass die Registrys für einige Domänen die Domäne sogar vor dem Ablaufdatum sperren.

Weitere Informationen zum Erneuern einer abgelaufenen Domäne finden Sie unter Verlängern der Registrierung für eine Domain.

Wir haben die Domäne aufgrund eines Verstoßes gegen die AWS Acceptable Use Policy gesperrt.

Wenn wir eine Domäne aufgrund eines Verstoßes gegen die AWS Acceptable Use Policy gesperrt haben, senden wir eine E-Mail-Benachrichtigung an den Registrierenden für die Domäne. (Wir senden keine Benachrichtigungs-E-Mail, wenn das AWS Konto bereits wegen Betrugs gesperrt wurde.)

Um eine Sperrung anzufechten, sende eine E-Mail an trustandsafety@support.aws.com.

Wir haben die Domäne aufgrund eines Gerichtsbeschlusses gesperrt.

Wenn eine Domäne aufgrund eines Gerichtsbeschlusses gesperrt wurde, können wir die Sperrung erst nach Aufhebung des Beschlusses rückgängig machen. Um die Gültigkeit eines Gerichtsbeschlusses anzufechten, senden Sie eine E-Mail an trustandsafety@support.aws.com und fügen Sie die entsprechenden Dokumente bei.

Mein Domainvorgang ist fehlgeschlagen

Hier finden Sie einige Tipps zur Fehlerbehebung, falls Ihr Domain-Betrieb fehlschlägt. Bei den Vorgängen kann es sich um Registrierung, Übertragung, Verlängerung oder Kontaktaktualisierung handeln.

Der Domainvorgang ist aufgrund ungültiger Kontaktinformationen fehlgeschlagen

Wenn ein Domainvorgang mit einer Fehlermeldung wegen ungültiger Kontaktinformationen fehlschlägt, entsprechen die von Ihnen angegebenen Kontaktdaten nicht den Validierungsanforderungen der Registry.

Um dieses Problem zu beheben, stellen Sie sicher, dass alle Kontaktdaten korrekt formatiert sind:

- Name — Stellen Sie sicher, dass der Name nur gültige Zeichen enthält und richtig formatiert ist.
- Adresse — Stellen Sie sicher, dass das Adressformat den Poststandards des Landes entspricht.
- Telefonnummer — Verwenden Sie das richtige internationale Format für das Land.
- Identifikationsfelder — Stellen Sie bei Domains, für die Identifikationsnummern erforderlich sind, sicher, dass das Format für das angegebene Land korrekt ist.

Nachdem Sie die Kontaktinformationen korrigiert haben, versuchen Sie den Domainvorgang erneut. Spezifische Anforderungen für verschiedene Top-Level-Domains finden Sie unterDomains, die Sie mit Amazon Route 53 registrieren können.

Übertragen meiner Domäne an Amazon Route 53 fehlgeschlagen

Wenn Ihre Domainübertragung bereits fehlgeschlagen ist oder abgelehnt wurde, verwenden Sie diesen Abschnitt, um den Fehler zu diagnostizieren und zu beheben.

> **Note**
>
> Informationen zur Vermeidung von Problemen bei aktiven Übertragungen finden Sie unterVermeidung häufiger Probleme bei der Übertragung von Route 53.

Themen

Sie haben nicht auf den Link in der Autorisierungs-E-Mail geklickt.

Wenn Sie eine Domainregistrierung an Amazon Route 53 übertragen, verlangt ICANN (das Verwaltungsorgan für die Domainregistrierung) eine Autorisierung für die Übertragung vom Registranten der Domain. Für diese Autorisierung senden wir Ihnen eine E-Mail mit einem Link. Sie haben je nach Top-Level-Domain zwischen 5 und 15 Tage Zeit, um auf den Link zu klicken. Nach dieser Zeit wird der Link funktionsunfähig.

Wenn Sie innerhalb der Frist nicht auf den Link in der E-Mail klicken, verlangt ICANN, dass wir die Übertragung abbrechen. Weitere Informationen dazu, wie die Autorisierungs-E-Mail erneut an den Registrierenden gesendet wird, finden Sie unter Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails.

Der Autorisierungscode, den Sie von der aktuellen Vergabestelle erhalten haben, ist nicht gültig.

Wenn Sie die Übertragung einer Domain in Amazon Route 53 beantragen, aber keine Autorisierungs-E-Mail erhalten, sehen Sie sich die Statusseite in der Route-53-Konsole an. Gehen Sie wie folgt vor, wenn die Statusseite zeigt, dass der von Ihrer Vergabestelle erhaltene Autorisierungscode für die Übertragung nicht gültig ist:

1. Wenden Sie sich an den aktuellen Registrierenden für die Domäne und fordern Sie einen neue Autorisierungscode an. Überprüfen Sie Folgendes:

   - Wie lange der neue Autorisierungscode aktiv bleibt. Sie müssen eine Domänenübertragung anfordern, bevor der Code abläuft.
   - Der neue Autorisierungscode unterscheidet sich vom nicht gültigen Code. Falls nicht, bitten Sie den aktuellen Registrierenden um eine Aktualisierung des Autorisierungscodes.

2. Senden Sie eine neue Anfrage zur Übertragung der Domäne. Weitere Informationen finden Sie unter Schritt 5: Anfordern der Übertragung im Thema Übertragen der Registrierung für eine Domain an Amazon Route 53.

Fehlermeldung „Parameter in Anforderung ungültig“ beim Versuch, eine .es-Domain an Amazon Route 53 zu übertragen

Amazon Route 53 gibt den Fehler „Parameter in Anforderung ungültig“ aus, wenn Sie versuchen, eine .es-Domain in Route 53 zu übertragen, und der Kontakttyp des Registranten-Kontakts ist Company (Unternehmen). Um die Übertragung abzuschließen, ändern Sie den Kontakttyp des Registranten in Person und senden Sie ihn erneut.

Ist der internationalisierte Domainname, den Sie an Amazon Route 53 übertragen, in Punycode aufgeführt?

Wenn Sie einen neuen Domänennamen registrieren oder gehostete Zonen und Datensätze erstellen, können Sie Zeichen aus anderen Alphabeten (z. B. Kyrillisch oder Arabisch) und Zeichen in chinesischer, japanischer oder koreanischer Schrift angeben. Amazon Route 53 speichert diese internationalisierten Domainnamen (IDNs) in Punycode, der Unicode-Zeichen als ASCII-Zeichenketten darstellt.

Wenn Sie bei der Übertragung einer an Route 53 eine Fehlermeldung erhalten, verwenden Sie Punycode, IDNs um diese darzustellen, und versuchen Sie es erneut. Weitere Informationen finden Sie unter Formatierung internationalisierter Domänennamen.

Häufige Fehlermeldungen bei der Übertragung

Wenn eine Domainübertragung fehlschlägt, erhalten Sie in der Regel entweder in der Route 53-Konsole oder per E-Mail eine Fehlermeldung. Hier sind die häufigsten Fehlermeldungen und wie Sie sie beheben können:

„Die Übertragung wurde von der Registry abgelehnt“

Dieser Fehler tritt auf, wenn die Domain-Registry die Übertragung aus einem von mehreren Gründen blockiert. Die häufigsten Ursachen sind:

- Die Domain entspricht nicht der 60-Tage-ICANN-Regel. Die ICANN verlangt, dass Übertragungen innerhalb von 60 Tagen nach der ersten Registrierung oder einer Änderung des Kontakts des Registranten blockiert werden.
- Für die Domain ist die Transfersperre bei Ihrem aktuellen Registrar aktiviert.
- Die Domain befindet sich in einem Status, der Übertragungen verhindert, z. B. `clientTransferProhibitedserverTransferProhibited`,, `pendingDeletependingTransfer`, oder`redemptionPeriod`.

Um dieses Problem zu lösen, erkundigen Sie sich bei Ihrem aktuellen Registrar nach den folgenden Fragen:

- Stellen Sie sicher, dass die Domain ab dem Datum der Registrierung mehr als 60 Tage alt ist. Wenn Sie kürzlich die Kontaktinformationen des Registranten geändert haben, müssen Sie nach dieser Änderung möglicherweise 60 Tage warten. Bei einigen Registraren können Sie diese Einschränkung deaktivieren. Fragen Sie daher Ihren aktuellen Registrar, ob diese Option verfügbar ist.
- Entsperren Sie die Domain, indem Sie alle Transfer- oder Domainsperren deaktivieren.
- Vergewissern Sie sich, dass Ihr Domainstatus Übertragungen zulässt. Sie können den Domainstatus mithilfe einer WHOIS-Suche überprüfen oder indem Sie sich an Ihren aktuellen Registrar wenden.

„Ungültiger Autorisierungscode“ oder „Authentifizierungscode ist falsch“

Dieser Fehler bedeutet, dass der von Ihnen eingegebene Autorisierungscode (auch EPP-Code oder Übertragungscode genannt) nicht gültig ist. Dies kann passieren, wenn der Code abgelaufen ist, falsch eingegeben wurde oder nicht von Ihrem aktuellen Registrar bezogen wurde.

So beheben Sie dieses Problem

- Wenden Sie sich an Ihren aktuellen Registrar, um einen neuen Autorisierungscode anzufordern. Fragen Sie unbedingt, wie lange der Code aktiv bleibt, damit Sie die Übertragung abschließen können, bevor er abläuft.
- Wenn Sie den neuen Code erhalten, vergewissern Sie sich, dass er sich vom vorherigen Code unterscheidet. Wenn es derselbe ist, bitten Sie Ihren Registrar, den Autorisierungscode zu aktualisieren oder neu zu generieren.

- Vergewissern Sie sich, dass Sie den Code genau wie angegeben eingeben, einschließlich aller Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

„Autorisierungs-E-Mail für die Übertragung nicht erhalten“ oder „Zeitlimit für die Autorisierung“

Dieser Fehler tritt auf, wenn Sie nicht innerhalb des erforderlichen Zeitraums (normalerweise 5 Tage) auf den Autorisierungslink in der Bestätigungs-E-Mail für die Übertragung klicken. ICANN verlangt diesen Autorisierungsschritt für alle Domainübertragungen.

Wenn Sie die Autorisierungs-E-Mail nicht erhalten oder die Frist verpasst haben, überprüfen Sie Folgendes:

- Überprüfe deinen Spam- oder Junk-E-Mail-Ordner. E-Mails zur Übertragungsautorisierung werden manchmal von E-Mail-Anbietern gefiltert.
- Vergewissern Sie sich, dass Ihr Postfach nicht voll ist und keine Speicherbeschränkungen bestehen, die die E-Mail-Zustellung verhindern könnten.
- Prüfen Sie, ob Ihr E-Mail-Anbieter Richtlinien hat, die eingehende E-Mails von unbekannten Absendern filtern.
- Vergewissern Sie sich, dass Sie auf das E-Mail-Konto des Registranten zugreifen können und dass die E-Mail-Adresse noch aktiv ist.

Falls erforderlich, aktualisieren Sie Ihre Kontaktinformationen bei Ihrem aktuellen Registrar, bevor Sie eine weitere Übertragung beantragen. Informationen zum erneuten Senden der Autorisierungs-E-Mail finden Sie unter. Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails

„Domain ist gesperrt“ oder „Übertragung verboten“

Dieser Fehler weist darauf hin, dass für Ihre Domain eine Sperre aktiviert ist, die Übertragungen verhindert. Die meisten Registrare aktivieren Domainsperren standardmäßig als Sicherheitsmaßnahme, um unbefugte Übertragungen zu verhindern.

Um dieses Problem zu beheben, melden Sie sich bei Ihrem aktuellen Registrar bei Ihrem Konto an und deaktivieren Sie die Einstellungen für die Domainsperre oder die Transfersperre. Die genauen Schritte variieren je nach Registrar, aber in der Regel finden Sie diese Einstellungen in Ihren Domainverwaltungs- oder Sicherheitseinstellungen. Wenn Sie Hilfe bei der Suche nach diesen Einstellungen benötigen, wenden Sie sich an Ihren aktuellen Registrar.

„Überprüfung der Kontaktinformationen erforderlich“

Dieser Fehler tritt auf, wenn Sie kürzlich die Kontaktinformationen Ihrer Domain geändert haben. Um betrügerische Übertragungen zu verhindern, sehen die ICANN-Regeln eine Wartezeit von 60 Tagen nach der Änderung des Kontakts vor, bevor eine Domain übertragen werden kann.

Um dieses Problem zu lösen, haben Sie zwei Möglichkeiten:

- Warten Sie 60 Tage ab dem Datum der Kontaktänderung, bevor Sie die Übertragung erneut versuchen.
- Wenden Sie sich an Ihren derzeitigen Registrar, um Ihre aktuellen Kontaktinformationen zu überprüfen. Bei einigen Registraren können Sie sich möglicherweise von der 60-Tage-Beschränkung abmelden, wenn Sie Ihre Identität überprüfen können.

> **Note**
>
> Wenn Sie eine Fehlermeldung erhalten, die hier nicht aufgeführt ist, wenden Sie sich an den AWS Support und geben Sie den genauen Fehlertext an. Unser Support-Team kann Ihnen helfen, Übertragungsprobleme zu diagnostizieren und zu lösen, die auf Ihre Situation zugeschnitten sind.

Ich habe DNS-Einstellungen geändert, diese sind aber nicht wirksam.

Wenn Sie DNS-Einstellungen geändert haben, finden Sie hier einige häufige Gründe dafür, warum die Änderungen noch nicht wirksam sind.

Themen

Sie haben den DNS-Dienst in der letzten 48 Stunden an Amazon Route 53 übertragen, weshalb DNS noch Ihren alten DNS-Dienst verwendet.

Als Sie den DNS-Dienst in Amazon Route 53 übertragen haben, haben Sie die von der Vergabestelle für Ihre Domain bereitgestellte Methode verwendet, um die Namenserver für den vorherigen DNS-Dienst mit den vier Namenservern für Route 53 zu ersetzen.

> **Note**
>
> Wenn Sie sich diesbezüglich nicht sicher sind, informieren Sie sich unter Sie haben den DNS-Dienst kürzlich an Amazon Route 53 übertragen, die Namenserver bei der Domainvergabestelle aber nicht aktualisiert..

Domänenvergabestellen arbeiten für gewöhnlich mit einem TTL-Zeitraum (Time-to-Live-Zeitraum) von 24 bis 48 Stunden für Namenserver. Das bedeutet, dass ein DNS-Resolver nach Abruf der Namenserver für Ihre Domäne diese Informationen bis zu 48 Stunden lang verwendet, bevor er eine andere Anfrage für die aktuellen Namenserver für die Domäne sendet. Wenn Sie den DNS-Dienst innerhalb der letzten 48 Stunden in Route 53 übertragen und dann die DNS-Einstellungen geändert haben, verwenden einige DNS-Resolver nicht Ihren alten DNS-Dienst für die Weiterleitung von Datenverkehr für die Domäne.

Sie haben den DNS-Dienst kürzlich an Amazon Route 53 übertragen, die Namenserver bei der Domainvergabestelle aber nicht aktualisiert.

Die Vergabestelle für Ihre Domäne verfügt über verschiedene Informationen zur Domäne, einschließlich der Namenserver für den DNS-Dienst für die Domäne. In der Regel ist die Domänenvergabestelle auch Ihr DNS-Dienst, weshalb die Namenserver Ihrer Domäne auch der Vergabestelle gehören. Diese Namenserver sagen DNS, wo Informationen zur Art und Weise der Datenverkehrsweiterleitung für Ihre Domäne abgerufen werden können, beispielsweise die IP-Adresse eines Webservers für Ihre Domäne.

Bei der Übertragung des DNS-Dienst an Amazon Route 53 müssen Sie die von Ihrer Domänenvergabestelle bereitgestellte Methode anwenden, um die mit Ihrer Domäne verbundenen Namenserver zu ändern. In der Regel ersetzen Sie die von der Vergabestelle bereitgestellten Namenserver mit den vier Route-53-Namenservern, die mit der gehosteten Zone verbunden sind, welche Sie für die Domäne erstellt haben.

Wenn Sie eine neue gehostete Zone und Datensätze für Ihre Domäne erstellt und andere Einstellungen als die für den vorherigen DNS-Dienst verwendeten festgelegt haben, und wenn DNS weiterhin Datenverkehr an die alten Ressourcen weiterleitet, haben Sie möglicherweise die Nameserver nicht bei der Domänenvergabestelle aktualisiert. Gehen Sie wie folgt vor, um zu ermitteln, ob die Vergabestelle die Namenserver für Ihre gehostete Route-53-Zone verwendet, und um gegebenenfalls die Namenserver für die Domäne zu aktualisieren:

Vorgehensweise zum Abrufen der Namenserver für Ihre gehostete Zone und zum Aktualisieren der Namenservereinstellung bei der Domänenvergabestelle

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones.
3. Wählen Sie auf der Seite Gehostete Zonen den Namen der gehosteten Zone (nicht das Optionsfeld) für die gehostete Zone aus.

   > **Important**
   >
   > Wenn Sie mehr als eine gehostete Zone mit demselben Namen haben, stellen Sie sicher, dass Sie die Namenserver für die richtige gehostete Zone abrufen.

4. Notieren Sie sich in der Liste Datensatzname die vier Server, die für Nameserver aufgeführt sind.
5. Zeigen Sie unter Verwendung der von der Vergabestelle für die Domäne bereitgestellten Methode die Liste der Namenserver für die Domäne an.
6. Wenn die Namenserver für die Domäne und Ihre Namenserver aus Schritt 4 übereinstimmen, ist die Domänenkonfiguration korrekt.

   Wenn die Namenserver für die Domäne und Ihre Namenserver aus Schritt 4 nicht übereinstimmen, müssen Sie die Domäne aktualisieren, sodass Route-53-Namenserver verwendet werden.
7.

> **Important**
>
> Wenn Sie die Namenserver für die Domäne ändern und die Namenserver Ihrer gehosteten Route-53-Zone einstellen, kann es bis zu zwei Tage dauern, bis die Änderung wirksam wird und Route 53 Ihr DNS-Dienst wird. Der Grund dafür ist, dass die DNS-Resolver im Internet

die Namenserver in der Regel nur einmal alle zwei Tage anfordern und die Antwort im Cache speichern.

DNS-Resolver verwenden immer noch die alten Einstellungen für den Datensatz.

Wenn Sie die Einstellungen in einem Datensatz geändert haben, aber der Datenverkehr immer noch zu den alten Ressourcen geleitet wird, beispielsweise zu einem Webserver für Ihre Website, ist ein möglicher Grund dafür, dass DNS nach wie vor die vorherigen Einstellungen im Cache gespeichert hat. Jeder Datensatz hat einen TTL-Wert (Time-to-Live-Wert), der angibt, wie lange (in Sekunden) DNS-Resolver Informationen im Datensatz im Cache speichern sollen, beispielsweise die IP-Adresse für einen Webserver. DNS-Resolver geben so lange den alten Wert bei DNS-Abfragen zurück, wie die vom TTL-Wert angegebene Zeit noch nicht abgelaufen ist. Gehen Sie wie folgt vor, wenn Sie ermitteln möchten, was der TTL-Wert für einen Datensatz ist.

> **Note**
>
> Bei Aliaseinträgen wird die TTL durch die AWS Ressource bestimmt, an die der Datensatz den Verkehr weiterleitet. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

So zeigen Sie die TTL für einen Datensatz an:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Wählen Sie auf der Seite Hosted Zones den Namen der gehosteten Zone aus, die den Datensatz enthält.
3. Suchen Sie in der Liste der Datensätze nach dem Datensatz, dessen TTL-Wert Sie ermitteln möchten, und sehen Sie sich den Wert in der Spalte TTL an.

   > **Note**
   >
   > Wenn Sie den TTL-Wert jetzt ändern, wird Ihre Änderung nicht schneller wirksam. DNS-Resolver haben den Wert bereits im Cache und rufen die neue Einstellung erst nach Ablauf der von der alten Einstellung vorgegebenen Zeit ab.

Sie haben mehr als eine gehostete Zone mit demselben Namen, und Sie haben diejenige aktualisiert, die nicht mit der Domäne verknüpft ist

Sie können mehr als eine gehostete Zone mit demselben Namen erstellen, entweder mit demselben Konto oder mit mehreren Konten. Um die gehostete Zone anzugeben, die Route 53 zum Weiterleiten des Internetdatenverkehrs für Ihre Domäne verwendet, rufen Sie die vier Route-53-Nameserver für diese gehostete Zone ab, und aktualisieren Sie die Domänenregistrierung, um diese Nameserver zu verwenden.

Wenn Sie Datensätze in einer gehosteten Zone hinzufügen, ändern oder löschen, Ihre Domänenregistrierung jedoch die Nameserver für eine andere gehostete Zone verwendet, werden die Route-53-Antworten auf DNS-Abfragen Ihre Änderungen nicht widerspiegeln. So ermitteln Sie, ob Ihre Domänenregistrierung die Nameserver für die gehostete Zone verwendet, in der Sie Datensätze aktualisiert haben:

1. Bestimmen Sie, welche Nameserver Ihrer Domänenregistrierung zugeordnet sind. Siehe Hinzufügen oder Ändern der Nameserver oder Glue-Datensätze.
2. Vergleichen Sie die Namenserver, die Sie in Schritt 1 erhalten haben, mit den Nameservern, die Route 53 der gehosteten Zone, in der Sie Datensätze aktualisiert haben, zugewiesen hat. Siehe Das Abrufen der Nameserver für eine öffentliche gehostete Zone.

Wenn die Namenserver für die Domänenregistrierung nicht mit den Namenservern für die gehostete Zone, in der Sie Datensätze aktualisiert haben, übereinstimmen, stehen Ihnen zwei Optionen zur Verfügung:

Ändern von Datensätzen in der gehosteten Zone, die derzeit der Domäne zugeordnet ist (empfohlen)

Notieren Sie sich die Änderungen, die Sie in der gehosteten Zone vorgenommen haben, die derzeit nicht mit Ihrer Domänenregistrierung verknüpft ist. Wechseln Sie dann zur gehosteten Zone, die mit der Domänenregistrierung verknüpft ist, und nehmen Sie die gleichen Änderungen vor. Dies ist die bevorzugte Methode, da die Änderungen fast sofort wirksam werden. Weitere Informationen finden Sie unter Bearbeiten von Datensätzen.

Aktualisieren Sie Ihre Domänenregistrierung, um andere Nameserver zu verwenden

Ändern Sie Ihre Domänenregistrierung, um die Nameserver in der gehosteten Zone, die Sie aktualisiert haben, zu verwenden.

> **Important**
>
> Wenn Sie die Nameserver ändern, die mit Ihrer Domänenregistrierung verknüpft sind, ist Ihre Domäne für bis zu 2 Tage nicht im Internet verfügbar. Dies liegt daran, dass DNS-Resolver in der Regel die Namen von Nameservern 2 Tage lang zwischenspeichern. Eine Übersicht über die Funktionsweise von DNS, einschließlich Informationen zum Zwischenspeichern der Auflösung finden Sie unter So leitet Amazon Route 53 Datenverkehr an Ihre Domain weiter.

Durch das Ändern der Nameserver, die mit Ihrer Domänenregistrierung verknüpft sind, ändern Sie im Wesentlichen den DNS-Dienst für die Domäne. Je nachdem, ob die Domäne derzeit verwendet wird, haben Sie zwei Möglichkeiten:

- Wird die Domäne derzeit verwendet, finden Sie unter Route 53 als DNS-Dienst für eine Domäne nutzen, die in Gebrauch ist weitere Informationen.
- Wenn die Domäne derzeit inaktiv ist, führen Sie die folgenden Aufgaben aus:
  1. Rufen Sie die Nameserver für die zu verwendende gehostete Zone ab, um den Datenverkehr an Ihre Domäne weiterzuleiten. Siehe Das Abrufen der Nameserver für eine öffentliche gehostete Zone.
  2. Vergewissern Sie sich in der gehosteten Zone, für die Sie Namenserver in Schritt 1 erhalten haben, dass der NS-Eintrag dieselben vier Namensserver verwendet. Wenn nicht, aktualisieren Sie den NS-Eintrag. Siehe Bearbeiten von Datensätzen.
  3. Aktualisieren Sie die Domänenregistrierung zur Verwendung der in Schritt 1 abgerufenen Namensserver: Siehe Hinzufügen oder Ändern der Nameserver oder Glue-Datensätze.

Mein Browser zeigt den Fehler "Server nicht gefunden" an.

Wenn Ihr Browser beim Versuch, zu einer Domäne (example.com) oder Subdomäne (www.example.com) zu navigieren, die Fehlermeldung "Server nicht gefunden" anzeigt, finden Sie hier gängige Erklärungen dafür.

Themen

- Sie haben keinen Datensatz für den Namen der Domäne oder Subdomäne erstellt.
- Sie haben einen Datensatz erstellt, aber den falschen Wert angegeben.
- Die Ressource, zu der Sie Datenverkehr weiterleiten, ist nicht verfügbar.

Sie haben keinen Datensatz für den Namen der Domäne oder Subdomäne erstellt.

Wenn Sie keinen Datensatz für die Domäne oder Subdomäne erstellen, weiß DNS nicht, wohin der Datenverkehr geleitet werden soll, wenn jemand diesen Namen in einen Browser eingibt. Weitere Informationen finden Sie unter Arbeiten mit Datensätzen.

Sie haben einen Datensatz erstellt, aber den falschen Wert angegeben.

Wenn Sie einen Datensatz erstellen, ist es leicht, den falschen Wert anzugeben, z. B. die IP-Adresse für einen Webserver oder den Domainnamen, CloudFront der Ihrer Webdistribution zugewiesen wurde. Wenn der Datensatz vorhanden ist, Sie aber dennoch die Fehlermeldung „Server nicht gefunden“ sehen, sollten Sie überprüfen, ob der Wert richtig ist.

Die Ressource, zu der Sie Datenverkehr weiterleiten, ist nicht verfügbar.

Wenn ein Datensatz eine Ressource angibt, wie zum Beispiel einen Webserver, der nicht verfügbar ist, gibt der Browser die Fehlermeldung „Server nicht gefunden“ zurück. Wir empfehlen, dass Sie den Status der Ressource überprüfen, zu der Sie Datenverkehr leiten.

Ich kann den Datenverkehr nicht an einen Amazon S3-Bucket leiten, der für Website-Hosting konfiguriert ist.

Wenn Sie einen Amazon-S3-Bucket für das Website-Hosting konfigurieren, müssen Sie dem Bucket denselben Namen wie dem Datensatz geben, den Sie für die Weiterleitung von Datenverkehr zum Bucket verwenden möchten. Wenn Sie beispielsweise den Datenverkehr für example.com zu einem S3-Bucket leiten möchten, der für Website-Hosting konfiguriert ist, muss der Name des Buckets example.com sein.

Wenn Sie Traffic an einen S3-Bucket weiterleiten möchten, der für das Hosting von Websites konfiguriert ist, aber der Name des Buckets nicht in der Alias-Zielliste der Amazon Route 53-Konsole erscheint, oder wenn Sie versuchen, einen Alias-Datensatz programmgesteuert zu erstellen, und Sie eine InvalidInput Fehlermeldung von der Route 53-API erhalten, überprüfen Sie eines der AWS SDKs AWS CLI, oder AWS Tools for Windows PowerShell, Folgendes:

- Der Name des Buckets stimmt genau mit dem Namen des Datensatzes überein, z. B. example.com oder www.example.com.

- Der S3-Bucket ist ordnungsgemäß für Website-Hosting konfiguriert. Weitere Informationen finden Sie unter Hosten von Websites auf Amazon S3 im Benutzerhandbuch für Amazon Simple Storage Service.

Mir wurden zweimal die Gebühren für eine gehostete Zone berechnet.

Wenn Sie eine gehostete Zone innerhalb von 12 Stunden nach ihrer Erstellung löschen, werden Ihnen dafür keine Gebühren in Rechnung gestellt. Nach 12 Stunden berechnen wir sofort die standardmäßige Monatsgebühr für eine gehostete Zone. Die monatliche Gebühr für eine gehostete Zone wird nicht anteilig für unvollständige Monate berechnet. (Die gleiche Gebühr fällt für die gehostete Zone an, die bei der Registrierung einer Domäne automatisch erstellt wird.)

Wenn Sie eine gehostete Zone am letzten Tag eines Monats erstellen, beispielsweise am 31. Januar, kann die Gebühr für Januar auf der Rechnung für den Februar erscheinen, zusammen mit der Gebühr für Februar. Beachten Sie, dass Amazon Route 53 mit der koordinierten Weltzeit (Universal Time Coordinated, UTC) als Zeitzone arbeitet, um zu ermitteln, wann eine gehostete Zone erstellt wurde.

Mir wurden mehrere Rechnungen für meine Domain berechnet

Wenn Sie sich für ein Abonnement registrieren, eine Anmeldegebühr, eine Überweisungsgebühr oder eine Verlängerungsgebühr mit Vorabkosten zahlen, wird eine eindeutige Rechnung erstellt. Diese Rechnung verbleibt in der Abrechnungskonsole, auch wenn die Zahlungstransaktion nicht erfolgreich ist. Der entsprechende Fakturierungsposten wird in der Fakturierungskonsole im Unterabschnitt Registrar-Global auf der Registerkarte Rechnungsdetails nach Service als [x] Menge angezeigt.

Gehen Sie wie folgt vor, um die Rechnungen einzusehen, auf die verzichtet wurde:

Um die Rechnungen, auf die verzichtet wurde, in der Abrechnungskonsole einzusehen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Fakturierung und Kostenmanagement Konsole unter https://console.aws.amazon.com/costmanagement/.
2. Wählen Sie im Navigationsbereich Rechnungen aus.
3. Wählen Sie Rechnungen aus, um Einzelheiten zu allen Rechnungen anzuzeigen, auf die verzichtet wurde.

Gehen Sie wie folgt vor, um die erfolgreichen Zahlungen und Rückerstattungen in der Abrechnungskonsole einzusehen:

Um die Zahlungen oder Rückerstattungen zu bestätigen, die erfolgreich verarbeitet wurden

1. Wählen Sie im Navigationsbereich Zahlungen aus.
2. Wählen Sie die Registerkarte Transaktionen, um die Tabelle Transaktionen für alle abgeschlossenen Transaktionen mit AWS anzuzeigen.

Mein AWS Konto ist geschlossen oder dauerhaft geschlossen und meine Domain ist bei Route 53 registriert

Wenn Sie Ihr AWS Konto schließen oder wenn Ihr Konto geschlossen oder dauerhaft geschlossen wird, werden Ihre Domains gelöscht:

1. Wir werden Sie darüber informieren, dass Ihr Konto geschlossen ist und Ihre Domain in den nächsten 5 Tagen täglich gesperrt wird.
2. Sobald Ihre Domain gesperrt ist, wird Folgendes geschehen:
   - Wenn Ihr Registrar Amazon Registrar ist, werden wir Sie darüber informieren, dass wir Ihre Domain innerhalb von 30 Tagen löschen werden. Weitere Informationen finden Sie unter Ihre Vergabestelle und andere Informationen zu Ihrer Domain finden.
   - Wenn Ihr Registrar Gandi ist, werden wir Sie darüber informieren, dass wir Ihre Domain für Gandi freigeben, sobald Ihr Konto dauerhaft geschlossen wird.
3. Nach einer Wartezeit von 30 Tagen löschen wir alle bei Amazon Registrar registrierten Domains im Konto und senden Ihnen ein Update.
4. Wenn Ihr Konto dauerhaft geschlossen wird, geben wir alle bei Gandi registrierten Domains in Ihrem Konto an Gandi weiter.

Wenn Sie Ihr Konto während des Zeitraums, in dem Ihre Domains wiederhergestellt werden können, erneut eröffnen, werden wir die Sperrung Ihrer Domains aufheben oder Sie darüber informieren, dass Ihre Domains gelöscht wurden, sie aber möglicherweise wiederhergestellt werden können. Weitere Informationen finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

> **Note**
>
> Sobald 90 Tage seit der Schließung Ihres Kontos vergangen sind, können Sie es nicht mehr erneut öffnen. Weitere Informationen finden Sie im Leitfaden zur Kontoverwaltung unter Ein Konto schließen.AWS

Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

IP-Adressbereiche von Amazon Route 53-Servern

Amazon Web Services (AWS) veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Wenn Ihre Firewalls oder Sicherheitsgruppen den eingehenden Datenverkehr auf Grundlage der Quell-IP-Adressen beschränkt, vergewissern Sie sich, dass Ihre Konfiguration den Datenverkehr von dem zutreffenden IP-Adressbereich zulässt.

Um die aktuellen IP-Adressbereiche für Route 53 anzuzeigen, laden Sie ip-ranges.json, herunter, und durchsuchen die Datei nach den folgenden Werten:

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

Weitere Informationen zu IP-Adressen für AWS Ressourcen finden Sie unter AWS IP-Adressbereiche im Allgemeine Amazon Web Services-Referenz.

IP-Adressbereiche von Route-53-Namenservern

`"service": "ROUTE53"`: Diese IP-Adressbereiche werden von Route-53-Namenservern verwendet. Fügen Sie diese Bereiche der Liste zulässiger IP-Adressbereiche hinzu, wenn Sie Route 53 als DNS-Service für eine oder mehrere Domänen verwenden und Sie die Befehle `dig` oder `nslookup` zum Abfragen von -Namensservern verwenden möchten.

> **Note**
>
> Die IP-Adressen der Route 53-Nameserver sind statisch.

IP-Adressbereiche von Route-53-Zustandsprüfungen

`"service": "ROUTE53_HEALTHCHECKS"`: Diese IP-Adressbereiche werden von Route-53-Zustandsprüfungen verwendet. Fügen Sie diese Bereiche zur Liste zulässiger IP-Adressbereiche hinzu, wenn Sie den Zustand der Ressourcen im Netzwerk mit Route 53-Zustandsprüfungen überprüfen.

> **Note**
>
> Wir ändern die IP-Adressbereiche von Health Checks selten. Überwachen Sie die Datei ip-ranges.json auf Aktualisierungen dieser Bereiche.

Weitere Informationen über IP-Adressen für Statusprüfungen finden Sie unter Konfigurieren von Router- und Firewall-Regeln für Amazon Route 53-Zustandsprüfungen.

Verweisen auf Präfixlisten

Bei einer Präfixliste handelt es sich um einen Satz mit mindestens einem CIDR-Blockeintrag, mit dem Sie Sicherheitsgruppen konfigurieren können. Ihr Router und Ihre Firewall für die Regeln für die EC2 Amazon-Instance müssen eingehenden Datenverkehr von den IP-Adressen zulassen, die die Route 53 53-Health Checker verwenden. Ein Verweis auf eine Präfixliste vereinfacht die Verwaltung der CIDR-Blöcke in Ihren Regeln. Wenn Sie häufig dasselbe für mehrere CIDRs Regeln verwenden, können Sie diese CIDRs in einer einzigen Präfixliste verwalten, anstatt CIDRs in jeder Regel wiederholt auf dasselbe zu verweisen. Wenn Sie einen CIDR-Block entfernen müssen, können Sie den zugehörigen Eintrag aus der Präfixliste entfernen, anstatt das CIDR aus jeder betroffenen Regel zu entfernen. Weitere Informationen zu Präfixlisten im Allgemeinen finden Sie im Amazon-VPC-Benutzerhandbuch unter Gruppieren von CIDR-Blöcken mit verwalteten Präfixlisten.

AWS-verwaltete Präfixlisten sind Gruppen von IP-Adressbereichen für AWS Dienste. AWS-verwaltete Präfixlisten werden von jedem Benutzer mit einem AWS Konto erstellt und verwaltet und können von diesen verwendet werden. AWS Sie können eine Liste mit AWS verwalteten Präfixen nicht erstellen, ändern, teilen oder löschen.

Weitere Informationen zu AWS-verwalteten Präfixlisten finden Sie unter Arbeiten mit AWS-verwalteten Präfixlisten im Amazon VPC-Benutzerhandbuch.

Interne IP-Adressbereiche von Route-53-Zustandsprüfungen

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`: Diese IP-Adressbereiche werden von Route 53 nur intern verwendet. Sie müssen diese Bereiche nicht der Liste der zulässigen Bereiche hinzufügen.

Amazon-Route-53-Ressourcen-Markierung

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jedes Tag besteht aus einem Schlüssel und einem Wert, die Sie beide selbst definieren. Der Schlüssel könnte beispielsweise „domain“ und der Wert „example.com“ lauten. Sie können Tags für verschiedene Zwecke nutzen; eine häufige Nutzung ist die Kategorisierung und Nachverfolgung der Amazon-Route-53-Kosten. Wenn Sie Tags auf von Route 53 gehostete Zonen, Domänen und Zustandsprüfungen anwenden, AWS generiert es einen Kostenverteilungsbericht als Datei mit kommagetrennten Werten (CSV), in der Ihre Nutzung und die Kosten nach Ihren Tags zusammengefasst sind. Sie können Tags anwenden, die geschäftliche Kategorien (wie Kostenstellen, Anwendungsnamen oder Eigentümer) darstellen, um die Kosten für mehrere Services zu organisieren. Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

Verwenden Sie den Tag-Editor in der, der eine zentrale, einheitliche Methode zur Erstellung und Verwaltung Ihrer Tags bietet AWS-Managementkonsole, um eine einfache Bedienung und optimale Ergebnisse zu erzielen. Weitere Informationen finden Sie unter Arbeiten mit dem Tag Editor in Erste Schritte mit der AWS-Managementkonsole. Sie können auch die Route-53-Konsole verwenden, um Tags für einige Ressourcen anzuwenden:

- Zustandsprüfungen – Weitere Informationen finden Sie unter Benennen und Verwenden von Tags für Zustandsprüfungen.
- Route 53 VPC Resolver eingehende Endpunkte — Weitere Informationen finden Sie unter. Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben
- Resolver-ausgehende Endpunkte – Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.
- Resolver-Regeln – Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.
- Gehostete Zonen – Weitere Informationen finden Sie unter Arbeiten mit gehosteten Zonen.

> **Note**
>
> Die Gebühren für Resolver-Endpunkte werden pro VPC Resolver-Netzwerkschnittstelle zugewiesen. Da es derzeit nicht möglich ist, VPC-Resolver-Netzwerkschnittstellen zu kennzeichnen, wird die tagbasierte Kostenzuweisung für Resolver-Endpunkte derzeit nicht

unterstützt. Informationen zu den Preisen für VPC Resolver finden Sie unter Amazon Route 53-Preise.

Sie können auch über die Route-53-API-Tags auf Ressourcen anwenden. Weitere Informationen finden Sie unter den Aktionen im Zusammenhang mit Tags im Thema Route-53-API-Aktionen nach Funktion in der Amazon-Route-53-API-Referenzaus.

Tutorials

In diesem Abschnitt werden die folgenden Tutorials behandelt:

Verwendung von Route 53 als DNS-Dienst für Subdomänen

Erfahren Sie, wie Sie Route 53 als DNS-Dienst für eine neue oder bestehende Subdomain verwenden und gleichzeitig einen anderen DNS-Dienst für die übergeordnete Domain verwenden.

Umstellung auf latenzbasiertes Routing

Erfahren Sie, wie Sie in Route 53 schrittweise vom Standardrouting zum latenzbasierten Routing migrieren und Benutzer zum Endpunkt mit der niedrigsten verfügbaren Latenz weiterleiten können. AWS

Kombinieren Sie Daten mit Gewichtung und Latenz für einen reibungslosen, risikoarmen Übergang mit voller Kontrolle und Rollback-Funktionalität.

Eine weitere Region zum latenzbasierten Routing hinzufügen

Erweitern Sie Ihr latenzbasiertes Routing-Setup, indem Sie eine neue AWS Region hinzufügen und den Verkehr schrittweise in die neue Region verlagern.

Weiterleitung des Datenverkehrs an mehrere EC2 Amazon-Instances in einer Region

Verwenden Sie eine Kombination aus Latenz und gewichteten Datensätzen, um den Datenverkehr an mehrere EC2 Amazon-Instances innerhalb einer bestimmten Instanz weiterzuleiten AWS-Region.

Verwaltung von über 100 gewichteten Datensätzen

Erfahren Sie, wie Sie Traffic an mehr als 100 Endpunkte weiterleiten können, indem Sie einen Baum aus gewichteten Aliasdatensätzen und gewichteten Datensätzen erstellen.

Gewichtung fehlertoleranter Antworten mit mehreren Datensätzen

Erfahren Sie, wie Sie DNS-Antworten, die mehrere Datensätze enthalten, gewichten und so für Fehlertoleranz und Lastenausgleich auf mehreren Endpunkten sorgen.

Diese Tutorials behandeln verschiedene Anwendungsfälle und Szenarien und helfen Ihnen dabei, die Routing-Richtlinien, gewichteten Datensätze und das latenzbasierte Routing von Route 53 effektiv zu nutzen, um Ihr DNS-Management und Ihr Traffic-Routing zu optimieren.

Themen

Verwendung von Amazon Route 53 als DNS-Service für eine Subdomäne ohne Migration der übergeordneten Domäne

Amazon Route 53 bietet Flexibilität bei der Verwaltung von DNS für Subdomains, sodass Sie die Funktionen nutzen können, ohne die gesamte übergeordnete Domain migrieren zu müssen.

Sie können entweder eine neue Subdomain erstellen oder eine bestehende auf Route 53 migrieren, während die übergeordnete Domain weiterhin bei einem anderen DNS-Dienstanbieter gehostet wird.

Eine neue Subdomain mit Route 53 erstellen:

1. Erstellen Sie eine gehostete Zone für die neue Subdomain.
2. Fügen Sie der Hosting-Zone die gewünschten DNS-Einträge (z. B. A, CNAME, MX) für die Subdomain hinzu.
3. Besorgen Sie sich die Route 53-Nameserver, die der Hosting-Zone zugewiesen sind.
4. Aktualisieren Sie die DNS-Konfiguration der übergeordneten Domäne, indem Sie NS-Einträge (Name Server) für die Subdomain hinzufügen, die auf die Route 53-Nameserver verweisen.

Migrieren einer vorhandenen Subdomain auf Route 53:

1. Erstellen einer gehosteten Zone für die Subdomäne.
2. Beziehen Sie die aktuelle DNS-Konfiguration für die Subdomain von Ihrem bestehenden DNS-Dienstanbieter.
3. Fügen Sie der Hosting-Zone die entsprechenden DNS-Einträge hinzu.

4. Besorgen Sie sich die Route 53-Nameserver, die der Hosting-Zone zugewiesen sind.
5. Aktualisieren Sie die DNS-Konfiguration der übergeordneten Domäne, indem Sie NS-Einträge für die Subdomain hinzufügen, die auf die Route 53-Nameserver verweisen.

Wenn Sie diese Schritte befolgen, können Sie die erweiterten Funktionen von Route 53 wie Integritätsprüfungen, Routing-Richtlinien und Verkehrsflussmanagement für Ihre Subdomänen nutzen und gleichzeitig die DNS-Konfiguration der übergeordneten Domain bei Ihrem bestehenden Anbieter beibehalten.

Themen

Erstellen einer Subdomäne, die Amazon Route 53 als DNS-Dienst verwendet, ohne die übergeordnete Domäne zu migrieren

Sie können eine Subdomäne erstellen, die Amazon Route 53 als DNS-Dienst verwendet, ohne die übergeordnete Domäne von einem anderen DNS-Dienst zu migrieren.

Der Vorgang umfasst folgende grundlegende Schritte:

1. Ermitteln Sie, ob Sie dieses Verfahren überhaupt anwenden sollten.
2. Erstellen einer gehosteten Route-53-Zone für die Subdomäne.
3. Fügen Sie Datensätze für die neue Subdomäne zu Ihrer gehosteten Route-53-Zone hinzu.
4. Nur API: Bestätigen Sie, dass Ihre Änderungen an alle Route-53-DNS-Server übertragen wurden.

> **Note**
>
> Derzeit besteht die einzige Möglichkeit, um zu überprüfen, ob Änderungen übernommen wurden, darin, die GetChangeAPI-Aktion zu verwenden. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route-53-Server übertragen.

5. Aktualisieren Sie den DNS-Dienst für die übergeordnete Domäne, indem Sie Namensserver-Datensätze für die Subdomäne hinzufügen.

Entscheidung über die Verfahren zum Erstellen einer Subdomäne

Die Verfahren in diesem Thema erläutern, wie Sie eine ungewöhnliche Operation durchführen. Wenn Sie Route 53 bereits als DNS-Dienst für Ihre Domain verwenden und lediglich den Traffic für eine Subdomain, z. B. www.example.com, an Ihre Ressourcen weiterleiten möchten, z. B. an einen Webserver, der auf einer EC2 Instance ausgeführt wird, finden Sie weitere Informationen unter. Weiterleiten von Datenverkehr für Subdomänen

Wenden Sie dieses Verfahren nur an, wenn Sie einen anderen DNS-Dienst für eine Domäne verwenden, z. B. example.com, und Route 53 als DNS-Dienst für eine neue Subdomäne dieser Domäne verwenden möchten, z. B. www.example.com.

Erstellen einer gehosteten Zone für die neue Subdomäne

Wenn Sie Amazon Route 53 als DNS-Dienst für eine neue Subdomäne verwenden möchten, ohne Migration der übergeordneten Domäne, erstellen Sie zunächst eine gehostete Zone für die Subdomäne. Route 53 speichert Informationen über Ihre Subdomäne in der gehosteten Zone.

Weitere Informationen zum Erstellen einer gehosteten Zone mithilfe der Route-53-Konsole finden Sie unter Erstellen einer öffentlichen gehosteten Zone.

Erstellen von Datensätzen

Sie können Datensätze entweder über die Amazon-Route-53-Konsole oder die Route-53-API erstellen. Die Datensätze, die Sie in Route 53 erstellen, werden von DNS verwendet, nachdem Sie die Verantwortlichkeit für die Subdomäne an Route 53 delegiert haben, wie im Abschnitt Aktualisieren des DNS-Dienst mit den Nameserver-Datensätzen für die Subdomäne unten erläutert.

> **Important**
>
> Erstellen Sie keine zusätzlichen Namensserver (NS)- oder Autoritätsursprung (SOA)-Datensätze in der gehosteten Route-53-Zone, und löschen Sie nicht die vorhandenen NS- und SOA-Datensätze.

Informationen zum Erstellen von Datensätzen mit der Route-53-Konsole finden Sie unter Arbeiten mit Datensätzen. Um Datensätze mit der Route-53-API zu erstellen, verwenden Sie `ChangeResourceRecordSets`. Weitere Informationen finden Sie ChangeResourceRecordSetsin der Amazon Route 53 API-Referenz.

Überprüfen des Status Ihrer Änderungen (nur API)

Die Verteilung der neuen gehosteten Zone und das Ändern der Datensätze auf die Route-53-DNS-Server nimmt etwas Zeit in Anspruch. Wenn Sie ChangeResourceRecordSetsfrüher Ihre Datensätze erstellt haben, können Sie anhand der `GetChange` Aktion feststellen, ob Ihre Änderungen übernommen wurden. (`ChangeResourceRecordSets`gibt einen Wert für zurück`ChangeId`, den Sie in eine nachfolgende `GetChange` Anforderung aufnehmen können. `ChangeId`dist nicht verfügbar, wenn Sie die Datensätze mit der Konsole erstellt haben.) Weitere Informationen finden Sie unter GET GetChange in der Amazon Route 53 API-Referenz.

> **Note**
>
> Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

Aktualisieren des DNS-Dienst mit den Nameserver-Datensätzen für die Subdomäne

Nachdem Ihre Änderungen an den Amazon-Route-53-Datensätzen weitergegeben wurden (siehe Überprüfen des Status Ihrer Änderungen (nur API)), aktualisieren Sie den DNS-Dienst für die übergeordnete Domäne, indem Sie NS-Datensätze für die Subdomäne hinzufügen. Dies wird als Delegieren der Verantwortlichkeit für die Subdomäne an Route 53 bezeichnet. Beispiel: Wenn die übergeordnete Domäne „example.com“ mit einem anderen DNS-Dienst gehostet wird und Sie die Subdomäne „test.example.com“ in Route 53 erstellt haben, müssen Sie den DNS-Dienst für „example.com“ mit neuen NS-Datensätzen für "test.example.com" aktualisieren.

Führen Sie die folgenden Schritte aus.

1. Sichern Sie mithilfe der Methode Ihres DNS-Dienstes die Zonendatei für die übergeordnete Domäne.
2. Rufen Sie in der Route-53-Konsole die Nameserver für Ihre gehostete Route-53-Zone ab:
   a. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
   b. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
   c. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone aus und wählen Sie dann View Details (Details anzeigen) aus.

d. Wählen Sie auf der Detailseite für die gehostete Zone Hosted Zone details (Details der gehosteten Zone) aus.

e. Notieren Sie sich die vier Server, die für Nameserver aufgeführt sind.

Sie können aber auch die `GetHostedZone`-Aktion verwenden. Weitere Informationen finden Sie GetHostedZonein der Amazon Route 53 API-Referenz.

3. Fügen Sie mithilfe der Methode Ihres DNS-Dienstes der übergeordneten Domäne NS-Datensätze für die Subdomäne zur Zonendatei für die übergeordnete Domäne hinzu. Geben Sie in diesen NS-Datensätzen die vier Route-53-Namensserver für die gehostete Zone an, die Sie in Schritt 1 erstellt haben.

> **Important**
>
> Fügen Sie keinen SOA-Datensatz zur Zonendatei für die übergeordnete Domäne hinzu. Da die Subdomäne Route 53 verwendet, hat der DNS-Dienst für die übergeordnete Domäne nicht die Autorität für die Subdomäne.
> Wenn Ihr DNS-Dienst automatisch einen SOA-Datensatz für die Subdomäne hinzugefügt hat, löschen Sie den Datensatz für die Subdomäne. Löschen Sie den SOA-Datensatz jedoch nicht für die übergeordnete Domäne.

Migration des DNS-Dienst für eine Subdomäne zu Amazon Route 53 ohne Migration der übergeordneten Domäne

Sie können eine Subdomäne migrieren, um Amazon Route 53 als DNS-Dienst zu verwenden, ohne die übergeordnete Domäne von einem anderen DNS-Dienst zu migrieren.

Der Vorgang umfasst folgende grundlegende Schritte:

1. Ermitteln Sie, ob Sie dieses Verfahren überhaupt anwenden sollten.
2. Erstellen einer gehosteten Route-53-Zone für die Subdomäne.
3. Rufen Sie die aktuelle DNS-Konfiguration vom aktuellen DNS-Dienstanbieter für die übergeordnete Domäne ab.
4. Fügen Sie Datensätze für die Subdomäne zu Ihrer gehosteten Route-53-Zone hinzu.
5. Nur API: Bestätigen Sie, dass Ihre Änderungen an alle Route-53-DNS-Server übertragen wurden.

> **Note**
>
> Derzeit besteht die einzige Möglichkeit, um zu überprüfen, ob Änderungen übernommen wurden, darin, die GetChangeAPI-Aktion zu verwenden. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

6. Aktualisieren Sie die DNS-Konfiguration mit dem DNS-Dienstanbieter für die übergeordnete Domäne, indem Sie Namenserver-Datensätze für die Subdomäne hinzufügen.

Entscheidung über die Verfahren zum Erstellen einer Subdomäne

Die Verfahren in diesem Thema erläutern, wie Sie eine ungewöhnliche Operation durchführen. Wenn Sie Route 53 bereits als DNS-Dienst für Ihre Domain verwenden und lediglich den Traffic für eine Subdomain, z. B. www.example.com, an Ihre Ressourcen weiterleiten möchten, z. B. an einen Webserver, der auf einer EC2 Instance ausgeführt wird, finden Sie weitere Informationen unter. Weiterleiten von Datenverkehr für Subdomänen

Wenden Sie dieses Verfahren nur an, wenn Sie einen anderen DNS-Dienst für eine Domäne verwenden, z. B. example.com und Route 53 als DNS-Dienst für eine vorhandene Subdomäne dieser Domäne verwenden möchten, z. B. www.example.com.

Erstellen einer gehosteten Zone für die Subdomäne

Wenn Sie eine Subdomäne von einem anderen DNS-Dienst zu Amazon Route 53 migrieren möchten, ohne die übergeordnete Domäne zu migrieren, müssen Sie zunächst eine gehostete Zone für die Subdomäne erstellen. Route 53 speichert Informationen über Ihre Subdomäne in der gehosteten Zone.

Weitere Informationen zum Erstellen einer gehosteten Zone mithilfe der Route-53-Konsole finden Sie unter Erstellen einer öffentlichen gehosteten Zone.

Abrufen Ihrer aktuellen DNS-Konfiguration von Ihrem DNS-Dienstanbieter

Zur Vereinfachung der Migration einer vorhandenen Subdomäne zu Route 53 müssen Sie die aktuelle DNS-Konfiguration für die Domäne vom DNS-Dienstanbieter abrufen, der aktuell den Dienst für die Domäne bereitstellt. Sie können diese Informationen als Grundlage für die Konfiguration von Route 53 als DNS-Dienst für die Subdomäne verwenden.

Was Sie abrufen und das Format, in dem es bereitgestellt wird, hängt davon ab, welches Unternehmen Sie derzeit als DNS-Dienstanbieter nutzen. Idealerweise erhalten Sie eine Zonendatei, die Informationen zu allen Datensätzen in Ihrer aktuellen Konfiguration enthält. (Datensätze teilen DNS mit, wie der Traffic für Ihre Domains und Subdomains weitergeleitet werden soll. Wenn beispielsweise jemand Ihren Domainnamen in einen Webbrowser eingibt, möchten Sie, dass der Datenverkehr an einen Webserver in Ihrem Rechenzentrum, an eine EC2 Amazon-Instance, an eine CloudFront Distribution oder an einen anderen Ort weitergeleitet wird?) Wenn es Ihnen möglich ist, eine Zonendatei von Ihrem aktuellen DNS-Dienstanbieter zu erhalten, können Sie die Zonendatei bearbeiten und die Datensätze entfernen, die Sie nicht zu Amazon Route 53 migrieren möchten. Anschließend können Sie die verbleibenden Datensätze in Ihre gehostete Route-53-Zone migrieren, wodurch der Prozess erheblich vereinfacht wird. Fragen Sie beim Kunden-Support für Ihren aktuellen DNS-Dienstanbieter nach, wie Sie eine Zonendatei oder eine Datensatzliste erhalten können.

Erstellen von Datensätzen

Verwenden Sie die von Ihrem aktuellen DNS-Dienstanbieter erhaltenen Datensätze als Ausgangspunkt, um entsprechende Datensätze in der gehosteten Amazon Route 53-Zone zu erstellen, die Sie für die Subdomäne erstellt haben. Die Datensätze, die Sie in Route 53 erstellen, werden von DNS verwendet, nachdem Sie die Verantwortlichkeit für die Subdomäne an Route 53 delegiert haben, wie im Abschnitt Aktualisieren des DNS-Dienst mit den Nameserver-Datensätzen für die Subdomäne unten erläutert.

> **Important**
>
> Erstellen Sie keine zusätzlichen Namensserver (NS)- oder Autoritätsursprung (SOA)-Datensätze in der gehosteten Route-53-Zone, und löschen Sie nicht die vorhandenen NS- und SOA-Datensätze.

Informationen zum Erstellen von Datensätzen mit der Route-53-Konsole finden Sie unter Arbeiten mit Datensätzen. Um Datensätze mit der Route-53-API zu erstellen, verwenden Sie `ChangeResourceRecordSets`. Weitere Informationen finden Sie ChangeResourceRecordSetsin der Amazon Route 53 API-Referenz.

Überprüfen des Status Ihrer Änderungen (nur API)

Die Verteilung der neuen gehosteten Zone und das Ändern der Datensätze auf die Route-53-DNS-Server nimmt etwas Zeit in Anspruch. Wenn Sie ChangeResourceRecordSetsfrüher Ihre Datensätze

erstellt haben, können Sie anhand der `GetChange` Aktion feststellen, ob Ihre Änderungen übernommen wurden. (`ChangeResourceRecordSets`gibt einen Wert für zurück`ChangeId`, den Sie in eine nachfolgende `GetChange` Anforderung aufnehmen können. `ChangeId`ist nicht verfügbar, wenn Sie die Datensätze mit der Konsole erstellt haben.) Weitere Informationen finden Sie unter GET GetChange in der Amazon Route 53 API-Referenz.

> **Note**
>
> Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Name-Server übertragen.

Aktualisieren des DNS-Dienst mit den Nameserver-Datensätzen für die Subdomäne

Nachdem Ihre Änderungen an den Amazon-Route-53-Datensätzen weitergegeben wurden (siehe Überprüfen des Status Ihrer Änderungen (nur API)), aktualisieren Sie den DNS-Dienst für die übergeordnete Domäne, indem Sie NS-Datensätze für die Subdomäne hinzufügen. Dies wird als Delegieren der Verantwortlichkeit für die Subdomäne an Route 53 bezeichnet. Angenommen, die übergeordnete Domäne example.com wird mit einem anderen DNS-Dienst gehostet und Sie migrieren die Subdomäne test.example.com zu Route 53. Erstellen Sie eine gehostete Zone für test.example.com und aktualisieren Sie den DNS-Dienst für example.com mit den NS-Datensätzen, die Route 53 der neuen gehosteten Zone für test.example.com zugeordnet hat.

Führen Sie die folgenden Schritte aus.

1. Sichern Sie mithilfe der Methode Ihres DNS-Dienstes die Zonendatei für die übergeordnete Domäne.
2. Wenn der vorherige DNS-Dienstanbieter für die Domäne eine Methode zum Ändern der TTL-Einstellungen für seine Namenserver hat, empfehlen wir, diese Einstellungen auf 900 Sekunden umzustellen. Dies begrenzt die Zeit, während der Client-Anforderungen versuchen, die Domänennamen mit veralteten Namensservern aufzulösen. Wenn der aktuelle TTL-Wert 172.800 Sekunden beträgt (also zwei Tage, was eine gängige Standardeinstellung ist), müssen Sie noch zwei Tage warten, bis Resolver und Clients keine DNS-Datensätze mit dem vorherigen TTL-Wert mehr im Cache haben. Nachdem die TTL-Einstellungen abgelaufen sind, können Sie die Datensätze beim vorherigen Anbieter löschen und Änderungen nur noch in Route 53 vornehmen.
3. Rufen Sie in der Route-53-Konsole die Nameserver für Ihre gehostete Route-53-Zone ab:

a. Melden Sie sich bei der Route 53-Konsole an AWS-Managementkonsole und öffnen Sie sie unter https://console.aws.amazon.com/route53/.

b. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

c. Wählen Sie auf der Seite Hosted Zones (Gehostete Zonen) das Optionsfeld (nicht den Namen) für die gehostete Zone aus und wählen Sie dann View Details (Details anzeigen) aus.

d. Wählen Sie auf der Detailseite für die gehostete Zone Hosted Zone details (Details der gehosteten Zone) aus.

e. Notieren Sie sich die vier Server, die für Nameserver aufgeführt sind.

Sie können aber auch die `GetHostedZone`-Aktion verwenden. Weitere Informationen finden Sie GetHostedZonein der Amazon Route 53 API-Referenz.

4. Fügen Sie mithilfe der Methode Ihres DNS-Dienstes der übergeordneten Domäne NS-Datensätze für die Subdomäne zur Zonendatei für die übergeordnete Domäne hinzu. Geben Sie den NS-Datensätzen denselben Namen wie der Subdomäne. Geben Sie in den NS-Datensätzen die vier Route-53-Namenserver für die gehostete Zone an, die Sie in Schritt 2 erstellt haben. Beachten Sie, dass unterschiedliche DNS-Dienste unterschiedliche Terminologie verwenden. Sie müssen eventuell den technischen Support für Ihren DNS-Dienst kontaktieren, um zu erfahren, wie Sie diesen Schritt durchführen.

   > **Important**
   >
   > Fügen Sie keinen SOA-Datensatz zur Zonendatei für die übergeordnete Domäne hinzu. Da die Subdomäne Route 53 verwendet, hat der DNS-Dienst für die übergeordnete Domäne nicht die Autorität für die Subdomäne.
   > Wenn Ihr DNS-Dienst automatisch einen SOA-Datensatz für die Subdomäne hinzugefügt hat, löschen Sie den Datensatz für die Subdomäne. Löschen Sie den SOA-Datensatz jedoch nicht für die übergeordnete Domäne.

   Abhängig von den TTL-Einstellungen für die Namensserver für die übergeordnete Domäne kann die Verteilung Ihrer Änderungen an die DNS-Auflöser 48 Stunden oder mehr dauern. Während dieses Zeitraums können DNS-Resolver immer noch mit den Namenservern für den DNS-Dienst der übergeordneten Domäne auf Anfragen antworten. Darüber hinaus können Client-Computer noch die vorherigen Namenserver für die Subdomäne in ihrem Cache haben.

5. Nachdem die TTL-Einstellungen der Vergabestelle für die Domäne abgelaufen sind (siehe Schritt 2), löschen Sie die folgenden Datensätze aus der Zonendatei für die übergeordnete Domäne:

   - Die Datensätze, die Sie zu Route 53 hinzugefügt haben, wie in Erstellen von Datensätzen beschrieben.
   - Die NS-Datensätze Ihres DNS-Dienstes. Nach dem Löschen der NS-Datensätze sind die einzigen NS-Datensätze in der Zonendatei diejenigen, die Sie in Schritt 4 erstellt haben.

Umstellung auf latenzbasiertes Routing in Amazon Route 53

Mit latenzbasiertem Routing kann Amazon Route 53 Ihre Benutzer zum Endpunkt mit der niedrigsten AWS verfügbaren Latenz weiterleiten. Sie können beispielsweise einen DNS-Namen `www.example.com` mit einem ELB Classic, einer Anwendung oder einem Network Load Balancer oder mit EC2 Amazon-Instances oder Elastic IP-Adressen verknüpfen, die in den Regionen USA Ost (Ohio) und Europa (Irland) gehostet werden. Die Route 53-DNS-Server entscheiden auf Basis der Netzwerkbedingungen der letzten beiden Wochen, welche Instances in welchen Regionen bestimmten Benutzern dienen sollen. Ein Benutzer in London wird wahrscheinlich zur Europa-(Irland)-Instance geleitet, ein Benutzer in Chicago zur USA-Ost-(Ohio)-Instance usw. Route 53 unterstützt latenzbasiertes Routing für A-, AAAA-, TXT- und CNAME-Datensätze sowie Aliasse für A- und AAAA-Datensätze.

> **Note**
>
> Daten über die Latenz zwischen Benutzern und Ihren Ressourcen basieren ausschließlich auf dem Verkehr zwischen Benutzern und AWS Rechenzentren. Wenn Sie in einer AWS Region keine Ressourcen verwenden, kann die tatsächliche Latenz zwischen Ihren Benutzern und Ihren Ressourcen erheblich von den AWS Latenzdaten abweichen. Dies gilt auch dann, wenn sich Ihre Ressourcen in derselben Stadt wie eine AWS Region befinden.

Für eine reibungslose, risikoarme Umstellung können Sie gewichtete und Latenz-Datensätze kombinieren, um nach und nach vom Standard-Routing zum latenzbasierten Routing zu migrieren, bei umfassender Kontrolle und mit Rollback-Möglichkeit in jeder Phase. Betrachten wir ein Beispiel, das `www.example.com` derzeit auf einer EC2 Amazon-Instance in der Region USA Ost (Ohio) gehostet wird. Die Instance hat die Elastic IP-Adresse `W.W.W.W`. Angenommen, Sie möchten gegebenenfalls weiterhin Traffic in die Region USA Ost (Ohio) weiterleiten und gleichzeitig damit

beginnen, Benutzer zu weiteren EC2 Amazon-Instances in der Region USA West (Nordkalifornien) (Elastic IP`X.X.X.X`) und in der Region Europa (Irland) (Elastic IP`Y.Y.Y.Y`) weiterzuleiten.
Die gehostete Route-53-Zone für `www.example.com` verfügt bereits über einen Datensatz für `example.com` mit Type (Typ) A und Value (Wert) (IP-Adresse) `W.W.W.W`.

Wenn Sie mit dem folgenden Beispiel fertig sind, verfügen Sie über zwei gewichtete Aliasdatensätze:

- Sie konvertieren Ihren vorhandenen Datensatz für `www.example.com` in einen gewichteten Alias-Datensatz, der weiterhin den Großteil Ihres Traffics an Ihre bestehende EC2 Amazon-Instance in der Region USA Ost (Ohio) weiterleitet.
- Sie erstellen einen anderen gewichteten Aliasdatensatz, der zu Beginn nur einen kleinen Teil Ihres Datenverkehrs zu Ihren Latenz-Datensätzen leitet, die Datenverkehr in alle drei Regionen leiten.

Durch die Aktualisierung der Gewichtungen in diesen gewichteten Aliasdatensätzen können Sie schrittweise von der Weiterleitung des Datenverkehrs nur in die Region USA Ost (Ohio) zur Weiterleitung von Datenverkehr an alle drei Regionen übergehen, in denen Sie EC2 Amazon-Instances haben.

Vorgehensweise zum Umstellen auf latenzbasiertes Routing

1. Kopieren Sie den Datensatz für `www.example.com`, verwenden Sie jedoch einen neuen Domänennamen, wie z. B. `copy-www.example.com`. Geben Sie dem neuen Datensatz denselben Type (A) und Value (`W.W.W.W`) wie dem Datensatz für `www.example.com`.
2. Aktualisieren Sie den vorhandenen A-Datensatz für `www.example.com`, um ihn zu einem gewichteten Aliasdatensatz zu machen:

   - Wählen Sie für Wert/Route-Datenverkehr nach Alias zu einem anderen Datensatz in dieser gehosteten Zone aus und geben Sie `copy-www.example.com` an.
   - Geben Sie für Gewicht 100 an.

   Wenn Sie mit der Aktualisierung fertig sind, verwendet Route 53 diesen Datensatz weiter, um sämtlichen Datenverkehr zu der Ressource mit der IP-Adresse `W.W.W.W` zu leiten.
3. Erstellen Sie einen Latenzdatensatz für jede Ihrer EC2 Amazon-Instances, zum Beispiel:

   - USA Ost (Ohio), Elastic-IP-Adresse `W.W.W.W`
   - USA West (Nordkalifornien), Elastic-IP-Adresse `X.X.X.X`
   - Europa (Irland), Elastic-IP-Adresse `Y.Y.Y.Y`

Geben Sie allen Latenz-Datensätzen denselben Domänennamen, beispielsweise `www-lbr.example.com`, und denselben Typ, A.

Nach dem Erstellen der Latenz-Datensätze leitet Route 53 weiterhin Datenverkehr unter Verwendung des in Schritt 2 aktualisierten Datensatzes weiter.

Sie können `www-lbr.example.com` für Validierungstests verwenden, um z. B. sicherzustellen, dass alle Endpunkte Anfragen akzeptieren können.

4. Fügen wir nun den `www-lbr.example.com` Latenzdatensatz zum `www.example.com` gewichteten Datensatz hinzu und beginnen, begrenzten Datenverkehr an die entsprechenden EC2 Amazon-Instances weiterzuleiten. Das bedeutet, dass die EC2 Amazon-Instance in der Region USA Ost (Ohio) Traffic von beiden gewichteten Datensätzen erhält.

   Erstellen Sie einen anderen gewichteten Aliasdatensatz für `www.example.com`:

   - Wählen Sie für Wert/Route-Datenverkehr nach Alias zu einem anderen Datensatz in dieser gehosteten Zone aus und geben Sie `www-lbr.example.com.` an.
   - Geben Sie für Gewicht 1 an.

   Wenn Sie fertig sind und Ihre Änderungen mit Route 53-Servern synchronisiert sind, leitet Route 53 einen winzigen Teil Ihres Datenverkehrs (1/101) an die EC2 Amazon-Instances weiter, für die Sie in Schritt 3 Latenzdatensätze erstellt haben.

5. Wenn Sie sich sicher sind, dass Ihre Endpunkte für den eingehenden Datenverkehr richtig skaliert sind, können Sie die Gewichtungen entsprechend anpassen. Wenn Sie beispielsweise möchten, dass 10 % Ihrer Anfragen auf latenzbasiertem Routing basieren, ändern Sie die Gewichtungen jeweils in 90 und 10.

Weitere Informationen zum Erstellen von Latenz-Datensätzen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

Hinzufügen einer anderen Region zu Ihrem latenzbasierten Routing in Amazon Route 53

Wenn Sie latenzbasiertes Routing verwenden und eine Instance in einer neuen Region hinzufügen möchten, können Sie Datenverkehr schrittweise zur neuen Region umstellen, genau wie Sie

den Datenverkehr in schrittweise auf latenzbasiertes Routing umgestellt haben Umstellung auf latenzbasiertes Routing in Amazon Route 53.

Angenommen, Sie verwenden latenzbasiertes Routing, um den Verkehr weiterzuleitenwww.example.com, und Sie möchten Ihren Instances in USA Ost (Ohio), USA West (Nordkalifornien) und Europa (Irland) eine EC2 Amazon-Instance im asiatisch-pazifischen Raum (Tokio) hinzufügen. Im folgenden Beispiel wird eine Möglichkeit zum Hinzufügen einer Instance in einer anderen Region erläutert.

In diesem Beispiel verfügt die gehostete Amazon-Route-53-Zone für `example.com` bereits über einen gewichteten Aliasdatensatz für `www.example.com`, der Datenverkehr zu den latenzbasierten Datensätzen für `www-lbr.example.com` weiterleitet:

- USA Ost (Ohio), Elastic-IP-Adresse `W.W.W.W`
- USA West (Nordkalifornien), Elastic-IP-Adresse `X.X.X.X`
- Europa (Irland), Elastic-IP-Adresse `Y.Y.Y.Y`

Der gewichtete Aliasdatensatz verfügt über eine Gewichtung von 100. Nehmen wir an, dass Sie nach dem Übergang zu latenzbasiertem Routing den anderen gewichteten Datensatz, den Sie für die Umstellung verwendet haben, gelöscht haben.

Vorgehensweise zum Hinzufügen einer anderen Region zu Ihrem latenzbasierten Routing in Route 53

1. Erstellen Sie vier neue latenzbasierte Datensätze, die die drei ursprünglichen Regionen sowie die neue Region umfassen, in die Sie ab jetzt Datenverkehr leiten möchten.

   - USA Ost (Ohio), Elastic-IP-Adresse `W.W.W.W`
   - USA West (Nordkalifornien), Elastic-IP-Adresse `X.X.X.X`
   - Europa (Irland), Elastic-IP-Adresse `Y.Y.Y.Y`
   - Asien-Pazifik (Tokio), Elastic-IP-Adresse`Z.Z.Z.Z`

   Geben Sie allen Latenz-Datensätzen denselben neuen Domänennamen, beispielsweise `www-lbr-2012-04-30.example.com`, und denselben Typ, A.

Nach dem Erstellen der Latenz-Datensätze leitet Route 53 weiterhin Datenverkehr unter Verwendung des ursprünglichen gewichteten Aliasdatensatzes (`www.example.com`) und der Latenz-Datensätze (`www-lbr.example.com`) weiter.

Sie können die Datensätze `www-lbr-2012-04-30.example.com` für Validierungstests verwenden, um beispielsweise sicherzustellen, dass alle Endpunkte Anfragen akzeptieren können.

2. Erstellen Sie einen gewichteten Aliasdatensatz für die neuen Latenz-Datensätze:

   - Geben Sie für den Domänennamen den Namen für den vorhandenen gewichteten Aliasdatensatz an: `www.example.com`.
   - Wählen Sie für Wert/Route-Datenverkehr nach Alias zu einem anderen Datensatz in dieser gehosteten Zone aus und geben Sie `www-lbr-2012-04-30.example.com` an.
   - Geben Sie für Gewicht 1 an.

   Wenn Sie fertig sind, leitet Route 53 einen winzigen Teil Ihres Datenverkehrs (1/101) an die EC2 Amazon-Instances weiter, für die Sie die `www-lbr-2012-04-30.example.com` Latenzdatensätze in Schritt 1 erstellt haben. Der Rest des Datenverkehrs wird weiterhin an die `www-lbr.example.com` Latenzdatensätze weitergeleitet, die die EC2 Amazon-Instance in der Region Asien-Pazifik (Tokio) nicht enthalten.

3. Wenn Sie sich sicher sind, dass Ihre Endpunkte für den eingehenden Datenverkehr richtig skaliert sind, können Sie die Gewichtungen entsprechend anpassen. Beispiel: Wenn Sie möchten, dass 10 % Ihrer Anfragen an die Latenz-Datensätze geleitet werden, die die Region Tokio umfassen, ändern Sie die Gewichtung für `www-lbr.example.com` von 100 in 90 und die Gewichtung für `www-lbr-2012-04-30.example.com` von 1 in 10.

Weitere Informationen zum Erstellen von Datensätzen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

Verwendung von Latenz und gewichteten Datensätzen in Amazon Route 53 zur Weiterleitung von Datenverkehr an mehrere EC2 Amazon-Instances in einer Region

Wenn Ihre Anwendung auf EC2 Amazon-Instances in zwei oder mehr EC2 Amazon-Regionen ausgeführt wird und Sie mehr als eine EC2 Amazon-Instance in einer oder mehreren Regionen haben, können Sie latenzbasiertes Routing verwenden, um den Datenverkehr an die richtige Region weiterzuleiten, und dann gewichtete Datensätze verwenden, um den Verkehr auf der Grundlage der von Ihnen angegebenen Gewichtungen an Instances innerhalb der Region weiterzuleiten.

Nehmen wir beispielsweise an, Sie haben drei EC2 Amazon-Instances mit Elastic IP-Adressen in der Region USA Ost (Ohio) und möchten Anfragen für Benutzer, für die USA Ost (Ohio) die geeignete Region ist, IPs gleichmäßig auf alle drei verteilen. In den anderen Regionen ist nur eine EC2 Amazon-Instance ausreichend, obwohl Sie dieselbe Technik auf viele Regionen gleichzeitig anwenden können.

Um Latenz und gewichtete Datensätze in Amazon Route 53 zu verwenden, um Traffic an mehrere EC2 Amazon-Instances in einer Region weiterzuleiten

1. Erstellen Sie eine Gruppe gewichteter Datensätze für die EC2 Amazon-Instances in der Region. Beachten Sie Folgendes:

   - Geben Sie allen gewichteten Datensätzen denselben Wert für Datensatzname (beispielsweise `us-east.example.com`) und Datensatztyp.
   - Wählen Sie für Wert-/Route-Verkehr zu IP-Adresse oder anderer Wert, abhängig vom Datensatztyp aus und geben Sie den Wert einer der Elastic-IP-Adressen an.
   - Wenn Sie die EC2 Amazon-Instances gleich gewichten möchten, geben Sie denselben Wert für Gewicht an.
   - Geben Sie bei Set ID (ID festlegen) für jeden Datensatz einen eindeutigen Wert an.

   Weitere Informationen zu Werten gewichteter Datensätze finden Sie unter Gewichtetes Routing.
2. Wenn Sie mehrere EC2 Amazon-Instances in anderen Regionen haben, wiederholen Sie Schritt 1 für die anderen Regionen. Geben Sie einen anderen Wert für Name in jeder Region an.
3. Erstellen Sie für jede Region, in der Sie mehrere EC2 Amazon-Instances haben (z. B. USA Ost (Ohio)), einen Latenz-Aliaseintrag. Wählen Sie für Wert/Route-Datenverkehr nach Alias für einen anderen Datensatz in dieser gehosteten Zone aus, und geben Sie den Wert des Felds

Datensatzname (z. B. `us-east.example.com`) an, den Sie den gewichteten Datensätzen in dieser Region zugewiesen haben.

4. Erstellen Sie für jede Region, in der Sie eine EC2 Amazon-Instance haben, einen Latenzdatensatz. Geben Sie für Datensatzname denselben Wert an, den Sie für die Latenz-Aliasdatensätze angegeben haben, die Sie in Schritt 3 erstellt haben. Wählen Sie für Value/Route traffic to die IP-Adresse oder einen anderen Wert, je nach Datensatztyp, und geben Sie die Elastic IP-Adresse der EC2 Amazon-Instance in dieser Region an.

   Weitere Informationen zum Hinzufügen von Alias-Datensätzen zu EC2 Amazon-Instances finden Sie unter Traffic an eine EC2 Amazon-Instance weiterleiten

Weitere Informationen zum Erstellen von Datensätzen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.

Verwalten von über 100 gewichteten Datensätzen in Amazon Route 53

In Amazon Route 53 können Sie gewichtete Datensätze konfigurieren. Sie können für einen bestimmten Namen und Typ (z. B. `www.example.com`, Typ A) bis zu 100 Alternativantworten konfigurieren, wobei jede ihre eigene Gewichtung hat. Beim Antworten auf Abfragen für `www.example.com` wählen Route-53-DNS-Server eine gewichtete Zufallsantwort aus, die an DNS-Resolver zurückgegeben wird. Der Wert eines gewichteten Datensatzes mit einer Gewichtung von 2 wird durchschnittlich zweimal so oft zurückgegeben wie der Wert eines gewichteten Datensatzes mit einer Gewichtung von 1.

Wenn Sie Datenverkehr an mehr als 100 Endpunkte leiten müssen, besteht eine Möglichkeit hierfür in der Verwendung eines Baums mit gewichteten Aliasdatensätzen und gewichteten Datensätzen. Das erste „Level” des Baums kann bis zu 100 gewichtete Alias-Datensätze beinhalten, die jeweils wiederum auf bis zu 100 gewichtete Datensätze verweisen können. Route 53 erlaubt bis zu drei Rekursionslevel, sodass Sie bis zu 1 000 000 eindeutige gewichtete Endpunkte verwalten können.

Ein einfacher Baum mit zwei Levels kann beispielsweise wie folgt aussehen:

Gewichtete Aliasdatensätze

- `www.example.com` verweist auf `www-a.example.com` mit einer Gewichtung von 1.
- `www.example.com` verweist auf `www-b.example.com` mit einer Gewichtung von 1.

Gewichtete Datensätze

- `www-a.example.com`, Typ A, Wert 192.0.2.1, Gewichtung 1
- `www-a.example.com`, Typ A, Wert 192.0.2.2, Gewichtung 1

- `www-b.example.com`, Typ A, Wert 192.0.2.3, Gewichtung 1
- `www-b.example.com`, Typ A, Wert 192.0.2.4, Gewichtung 1

Weitere Informationen zum Erstellen von Datensätzen finden Sie unter Arbeiten mit Datensätzen.

Gewichtung von fehlertoleranten Antworten mit mehreren Datensätzen in Amazon Route 53

> **Note**
>
> Das Verhalten von Datensätzen, die die mehrwertige Antwort-Routing-Richtlinie verwenden, ist in vielerlei Hinsicht dem Verhalten der in diesem Tutorial dokumentierten Konfiguration ähnlich. Der wesentliche Unterschied besteht darin, dass die Tutorial-Konfiguration es Ihnen erlaubt, Gewichtungen anzugeben, was hilfreich sein kann, wenn Ihre Endpunkte unterschiedliche Kapazitäten haben. Weitere Informationen finden Sie unter Mehrwertiges Antwort-Routing.

Ein gewichteter Amazon-Route-53-Datensatz kann nur mit einem Datensatz verbunden werden, also mit einer Kombination aus einem Namen (z. B. `example.com`) und einem Datensatztyp (z. B. A). Es ist aber oft wünschenswert, DNS-Antworten, die mehrere Datensätze enthalten, eine Gewichtung zuzuweisen.

Sie könnten beispielsweise acht EC2 Amazon-Instances oder Elastic IP-Endpunkte für einen Service haben. Wenn die Clients dieses Services erneute Verbindungsversuche unterstützen (wie alle gängigen Browser), dann werden diesen Clients durch Bereitstellung mehrerer IP-Adressen in DNS-Antworten alternative Endpunkte zur Verfügung gestellt, falls es bei einem bestimmten Endpunkt zu einem Ausfall kommt. Sie können sich sogar vor dem Ausfall einer Availability Zone schützen, wenn Sie Antworten so konfigurieren, dass sie eine Mischung aus in zwei oder mehr Availability Zones IPs gehosteten Komponenten enthalten.

Multi-Datensatz-Antworten sind auch nützlich, wenn eine große Anzahl von Clients (z. B. mobile Webanwendungen) sich wenige DNS-Caches teilen. In diesem Fall ermöglichen Multi-Datensatz-Antworten Clients das Senden von Anfragen an mehrere Endpunkte, auch wenn sie eine allgemeine DNS-Antwort vom gemeinsam genutzten Cache erhalten.

Diese Arten von gewichteten Multi-Datensatz-Antworten werden mittels einer Kombination von Datensätzen und gewichteten Aliasdatensätzen erreicht. Sie können acht Endpunkte in zwei verschiedene Datensätze mit jeweils vier IP-Adressen aufteilen:

`endpoint-a.example.com`, Typ A, mit den folgenden Werten:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, Typ A, mit den folgenden Werten:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

Sie können dann einen gewichteten Aliasdatensatz erstellen, der auf die einzelnen Gruppen verweist:

- `www.example.com` verweist auf `endpoint-a.example.com`, Typ A, Gewichtung 1
- `www.example.com` verweist auf `endpoint-b.example.com`, Typ A, Gewichtung 1

Weitere Informationen zum Erstellen von Datensätzen finden Sie unter Arbeiten mit Datensätzen.

Bewährte Methoden für Amazon Route 53

Dieser Abschnitt enthält bewährte Methoden für verschiedene Komponenten von Amazon Route 53, darunter:

1. Bewährte Methoden für DNS:
   - Machen Sie sich mit den Kompromissen zwischen TTL-Werten (Time to Live) und Reaktionsfähigkeit und Zuverlässigkeit vertraut.
   - Verwenden Sie nach Möglichkeit Alias-Datensätze anstelle von CNAME-Datensätzen, um die Leistung zu verbessern und Kosten zu sparen.
   - Konfigurieren Sie Standard-Routing-Richtlinien, um sicherzustellen, dass alle Clients eine Antwort erhalten.
   - Nutzen Sie latenzbasiertes Routing zur Minimierung der Anwendungslatenz und geolocation/ geoproximity Routing für Stabilität und Vorhersehbarkeit.
   - Überprüfen Sie die Weitergabe von Änderungen mithilfe der `GetChange` API für automatisierte Workflows.
   - Delegieren Sie Subdomänen aus der übergeordneten Zone, um ein konsistentes Routing zu gewährleisten.
   - Vermeiden Sie große Einzelantworten, indem Sie das Routing mehrwertiger Antworten verwenden.
2. Bewährte Methoden für Resolver:
   - Vermeiden Sie Routingschleifen, indem Sie vermeiden, dieselbe VPC sowohl einer Resolver-Regel als auch ihrem eingehenden Endpunkt zuzuordnen.
   - Implementieren Sie Sicherheitsgruppenregeln, um den Aufwand für die Verbindungsverfolgung zu reduzieren und den Abfragedurchsatz zu maximieren.
   - Konfigurieren Sie eingehende Endpunkte mit IP-Adressen in mehreren Availability Zones, um Redundanz zu gewährleisten.
   - Seien Sie sich möglicher DNS-Zone-Walking-Angriffe bewusst und wenden Sie sich an den AWS Support, wenn Ihre Endgeräte gedrosselt werden.
3. Bewährte Verfahren für Gesundheitschecks:
   - Folgen Sie den Empfehlungen zur Optimierung von Amazon Route 53 53-Zustandsprüfungen, um eine zuverlässige Überwachung Ihrer Ressourcen zu gewährleisten

Wenn Sie sich an diese bewährten Methoden halten, können Sie die Leistung, Zuverlässigkeit und Sicherheit Ihrer DNS-Infrastruktur optimieren und so eine effiziente und effektive Weiterleitung des Datenverkehrs zu Ihren Anwendungen und Diensten sicherstellen

Themen

Bewährte Methoden für Amazon Route 53 DNS

Befolgen Sie diese bewährten Methoden, um bei der Verwendung des DNS-Dienstes von Amazon Route 53 beste Ergebnisse zu erzielen.

Verwenden Sie die Datenebenenfunktionen für DNS Failover und Anwendungswiederherstellung

Die Datenebenen für Route 53, einschließlich Zustandsprüfungen und Amazon Application Recovery Controller (ARC) -Routing-Steuerung, sind weltweit verteilt und auf hundertprozentige Verfügbarkeit und Funktionalität ausgelegt, selbst bei schwerwiegenden Ereignissen. Sie integrieren sich miteinander und hängen nicht von der Funktionalität der Steuerebene ab. Die Steuerebenen für diese Dienste, einschließlich ihrer Konsolen, sind zwar im Allgemeinen sehr zuverlässig, sie sind aber zentralisierter konzipiert und priorisieren Beständigkeit und Konsistenz anstelle von hoher Verfügbarkeit. Für Szenarien wie ein Failover während der Notfallwiederherstellung empfehlen wir die Verwendung von Funktionen wie Route 53-Zustandsprüfungen und ARC-Routing-Steuerung, die zur DNS-Aktualisierung auf Datenebenenfunktionen angewiesen sind. Weitere Informationen finden Sie unter Konzepte für Steuer- und Datenebene und im Blog: Erstellen von Notfallwiederherstellungsmechanismen mit Amazon Route 53.

Auswählen von TTL-Werten für DNS-Datensätze

Die DNS-TTL ist der numerische Wert (in Sekunden), mit dem DNS-Resolver entscheiden, wie lange ein Datensatz zwischengespeichert werden kann, ohne eine weitere Abfrage an Route 53 zu stellen. Für alle DNS-Datensätze muss eine TTL angegeben sein. Der empfohlene Bereich für TTL-Werte beträgt 60 bis 172 800 Sekunden.

Die Wahl einer TTL ist ein Kompromiss zwischen Latenz und Zuverlässigkeit auf der einen und Reaktionsfähigkeit auf Änderungen auf der anderen Seite. Bei kürzeren TTLs Einträgen

stellen DNS-Resolver Aktualisierungen des Datensatzes schneller fest, da sie häufiger Abfragen durchführen müssen. Dies erhöht das Abfragevolumen (und die Kosten). Wenn Sie die TTL verlängern, beantworten DNS-Resolver häufiger Abfragen aus dem Cache, was normalerweise schneller, günstiger und in einigen Situationen zuverlässiger ist, da die Abfragen nicht aus dem Internet vorgenommen werden. Es gibt keinen richtigen Wert, aber Sie sollten sich fragen, ob Reaktionsfähigkeit oder Zuverlässigkeit für Sie wichtiger ist.

Beachten Sie folgende Punkte beim Festlegen von TTL-Werten:

- Richten Sie den DNS-Eintrag TTLs so lange ein, wie Sie es sich leisten können, auf das Inkrafttreten einer Änderung zu warten. Dies gilt insbesondere für Delegierungen (NS-Datensätze) oder andere Datensätze, die sich selten ändern, z. B. MX-Datensätze. Für diese Einträge wird ein längerer TTLs Zeitraum empfohlen. Die meisten werden auf eine Dauer zwischen einer Stunde (3 600 Sekunden) und einem Tag (86 400 Sekunden) festgelegt.
- Für Datensätze, die im Rahmen eines schnellen Failover-Mechanismus geändert werden müssen (insbesondere Datensätze, deren Integrität überprüft wurde), TTLs sind niedrigere Werte angemessen. Das Festlegen einer TTL von 60 oder 120 Sekunden ist eine übliche Wahl für dieses Szenario.
- Wenn Sie Änderungen an wichtigen DNS-Einträgen vornehmen möchten, empfehlen wir Ihnen, den TTLs vorübergehend zu kürzen. Dann können Sie die Änderungen vornehmen, beobachten und bei Bedarf schnell zurücksetzen. Sobald die Änderungen abgeschlossen sind und wie erwartet funktionieren, können Sie die TTL verlängern.

Weitere Informationen finden Sie unter TTL (Sekunden).

CNAME-Datensätze

CNAME-Datensätze sind eine Möglichkeit, mit einem Domänennamen auf einen anderen zu verweisen. Wenn ein DNS-Resolver domain-1.example.com auflöst und einen CNAME findet, der auf domain-2.example.com verweist, muss der DNS-Resolver domain-2.example.com auflösen, bevor er antworten kann. Diese Datensätze sind in vielen Situationen nützlich, um beispielsweise die Konsistenz zu gewährleisten, wenn eine Website mehr als einen Domänennamen hat.

DNS-Resolver müssen jedoch mehr Anfragen stellen, um sie zu beantworten CNAMEs, was die Latenz und die Kosten erhöht. Wenn möglich, besteht eine schnellere und günstigere Alternative darin, einen Route-53-Alias-Datensatz zu verwenden. Aliaseinträge ermöglichen es Route 53, mit einer direkten Antwort für AWS Ressourcen (z. B. einen Load Balancer) und für andere Domänen innerhalb derselben Hostzone zu antworten.

Weitere Informationen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Erweiterte DNS-Weiterleitung

- Wenn Sie Geolokalisierung, Geoproximity oder latenzbasiertes Routing verwenden, legen Sie immer einen Standardwert fest, es sei denn, Sie möchten, dass einige Kunden die Antwort no answer (keine Antwort) erhalten.
- Verwenden Sie latenzbasiertes Routing, um die Anwendungslatenz zu minimieren. Diese Art der Datenweiterleitung kann sich häufig ändern.
- Um Routingstabilität und Planbarkeit zu gewährleisten, verwenden Sie entweder Geolokalisierung oder Geoproximity-Routing.

Weitere Informationen finden Sie unter Geolocation-Routing, Geoproximity-Routing und Latenzbasiertes Routing.

DNS-Änderungsverbreitung

Wenn Sie einen Datensatz oder eine gehostete Zone mithilfe der Route-53-Konsole oder -API erstellen oder aktualisieren, dauert es einige Zeit, bis die Änderung im Internet sichtbar wird. Das wird Verbreitung von Änderungen genannt. Während die Verbreitung weltweit für gewöhnlich weniger als eine Minute dauert, gibt es gelegentlich Verzögerungen, z. B. aufgrund von Problemen bei der Synchronisierung mit einem Standort oder, in seltenen Fällen, aufgrund von Problemen innerhalb der zentralen Steuerebene. Wenn Sie automatisierte Bereitstellungs-Workflows erstellen und es wichtig ist, zu warten, bis die Übertragung der Änderungen abgeschlossen ist, bevor Sie mit dem nächsten Workflow-Schritt fortfahren, überprüfen Sie mithilfe der GetChangeAPI, ob Ihre DNS-Änderungen wirksam geworden sind ()`Status =INSYNC`.

DNS-Delegierung

Wenn Sie mehrere Subdomänen-Ebenen in DNS delegieren, ist es wichtig, immer von der übergeordneten Zone, der „parent“-Zone, aus zu delegieren. Wenn Sie beispielsweise www.dept.example.com delegieren, sollten Sie dies aus der Zone dept.example.com und nicht aus der Zone example.com tun. Delegierungen von einer grandparent- zu einer child-Zone funktionieren möglicherweise überhaupt nicht oder nur inkonsistent. Weitere Informationen finden Sie unter Weiterleiten von Datenverkehr für Subdomänen.

Größe der DNS-Antwort

Erstellen Sie keine großen Einzelantworten. Bei einer Größe von über 512 Byte müssen viele DNS-Resolver erneute Versuche über TCP anstelle von UDP ausführen, was zu langsameren

Antworten und geringerer Zuverlässigkeit führen kann. Wir empfehlen die Verwendung von Antworten mit mehreren Werten, die acht gesunde, zufällige IPs auswählen, damit die Antworten innerhalb der 512-Byte-Grenze bleiben.

Weitere Informationen finden Sie unter Mehrwertiges Antwort-Routing sowie unter DNS-Antwortgröße-Testserver.

Bewährte Methoden für VPC Resolver

Dieser Abschnitt enthält bewährte Methoden für die Optimierung von Amazon Route 53 VPC Resolver und behandelt die folgenden Themen:

1. Vermeidung von Loop-Konfigurationen mit Resolver-Endpunkten:
   - Vermeiden Sie Routingschleifen, indem Sie sicherstellen, dass dieselbe VPC nicht sowohl mit einer Resolver-Regel als auch mit ihrem eingehenden Endpunkt verknüpft ist.
   - Verwenden Sie diese AWS RAM Option für die gemeinsame Nutzung VPCs durch mehrere Konten unter Beibehaltung der korrekten Routing-Konfigurationen.

   Weitere Informationen finden Sie unter Vermeiden SieSchleifenkonfigurationenResolver-Endpunkt.
2. Skalierung von Resolver-Endpunkten:
   - Implementieren Sie Sicherheitsgruppenregeln, die den Datenverkehr auf der Grundlage des Verbindungsstatus zulassen, um den Aufwand für die Verbindungsverfolgung zu reduzieren
   - Befolgen Sie die empfohlenen Sicherheitsgruppenregeln für eingehende und ausgehende Resolver-Endpunkte, um den Abfragedurchsatz zu maximieren.
   - Überwachen Sie eindeutige Kombinationen von IP-Adressen und Ports, die DNS-Verkehr generieren, um Kapazitätsbeschränkungen zu vermeiden.

   Weitere Informationen finden Sie unter Resolver-Endpunkt-Skalierung.
3. Hohe Verfügbarkeit für Resolver-Endpunkte:
   - Erstellen Sie aus Redundanzgründen eingehende Endpunkte mit IP-Adressen in mindestens zwei Availability Zones.
   - Stellen Sie zusätzliche Netzwerkschnittstellen bereit, um die Verfügbarkeit bei Wartungsarbeiten oder bei hohem Datenaufkommen sicherzustellen

   Weitere Informationen finden Sie unter Hohe Verfügbarkeit für Resolver-Endpunkt .
4. Verhinderung von DNS-Zone-Walking-Angriffen:

- Seien Sie sich möglicher DNS-Zone-Walking-Angriffe bewusst, bei denen Angreifer versuchen, den gesamten Inhalt aus DNSSEC-signierten DNS-Zonen abzurufen.
- Wenn Ihre Endgeräte aufgrund des vermuteten Zonenwechsels gedrosselt werden, wenden Sie sich an den Support, um AWS Unterstützung zu erhalten.

Weitere Informationen finden Sie unter Gehen Sie zur DNS-Zone .

Wenn Sie diese bewährten Methoden befolgen, können Sie die Leistung, Skalierbarkeit und Sicherheit Ihrer VPC-Resolver-Bereitstellungen optimieren und so eine zuverlässige und effiziente DNS-Auflösung für Ihre Anwendungen und Ressourcen sicherstellen.

Vermeiden SieSchleifenkonfigurationenResolver-Endpunkt

Ordnen Sie dieselbe VPC nicht einer Resolver-Regel und ihrem eingehenden Endpunkt zu (unabhängig davon, ob es sich um ein direktes Ziel des Endpunkts oder über einen On-Premises-DNS-Server handelt). Wenn der ausgehende Endpunkt in einer Resolver-Regel auf einen eingehenden Endpunkt verweist, der eine VPC mit der Regel gemeinsam verwendet, kann dies zu einer Schleife führen, in der die Abfrage kontinuierlich zwischen den eingehenden und ausgehenden Endpunkten übergeben wird.

Die Weiterleitungsregel kann mithilfe von AWS Resource Access Manager (AWS RAM) weiterhin mit anderen Konten verknüpft werden VPCs , die mit anderen Konten geteilt wurden. Private gehostete Zonen, die dem Hub oder einer zentralen VPC zugeordnet sind, werden weiterhin von Abfragen an eingehende Endpunkte aufgelöst, da eine Weiterleitungsauflösungsregel diese Auflösung nicht ändert.

Resolver-Endpunkt-Skalierung

Resolver-Endpunkt Sicherheitsgruppen verwenden die Verbindungsverfolgung zum Sammeln von Informationen über Datenverkehr zu und von den Endpunkten. Jede Endpunktschnittstelle verfügt über eine maximale Anzahl von Verbindungen, die verfolgt werden können, und eine hohe Anzahl von DNS-Abfragen kann die Verbindungen überschreiten und zu Drosselung und Abfrageverlust führen. Die Verbindungsverfolgung AWS ist das Standardverhalten zur Überwachung des Datenverkehrs, der durch Sicherheitsgruppen fließt (SGs). Durch die Verwendung der Verbindungsverfolgung SGs wird der Durchsatz des Datenverkehrs reduziert. Sie können jedoch Verbindungen ohne Nachverfolgung implementieren, um den Overhead zu reduzieren und die Leistung zu verbessern. Weitere Informationen finden Sie unter Verbindungen ohne Nachverfolgung.

Wenn die Verbindungsverfolgung entweder mithilfe restriktiver Sicherheitsgruppenregeln erzwungen wird oder Abfragen über den Network Load Balancer weitergeleitet werden (siehe Automatisch verfolgte Verbindungen), kann die maximale Gesamtzahl der Abfragen pro Sekunde und IP-Adresse für einen Endpunkt bis zu 1500 betragen.

Regelempfehlungen für Sicherheitsgruppen für eingehenden und ausgehenden Datenverkehr für den Resolver-Endpunkt für eingehende Anrufe

Regeln für eingehenden Datenverkehr

Protokolltyp	Port-Nummer	Quell-IP
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

Regeln für ausgehenden Verkehr

Protokolltyp	Port-Nummer	Ziel-IP
TCP	Alle	0.0.0.0/0
UDP	Alle	0.0.0.0/0

Empfehlungen für Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr für den Outbound-Resolver-Endpunkt

Regeln für eingehenden Datenverkehr

Protokolltyp	Port-Nummer	Quell-IP
TCP	Alle	0.0.0.0/0
UDP	Alle	0.0.0.0/0

Regeln für ausgehenden Verkehr

Protokolltyp	Port-Nummer	Ziel-IP
TCP	53	0.0.0.0/0

UDP	53	0.0.0.0/0

> **Note**
>
> Port-Anforderungen für Sicherheitsgruppen:
>
> - Für eingehende Endpunkte sind Eingangsregeln erforderlich, die es TCP und UDP auf Port 53 ermöglichen, DNS-Anfragen von Ihrem Netzwerk zu empfangen. Ausgangsregeln können alle Ports zulassen, da der Endpunkt möglicherweise auf Anfragen von verschiedenen Quellports antworten muss.
> - Für ausgehende Endpunkte sind Ausgangsregeln erforderlich, die den TCP- und UDP-Zugriff auf die Ports ermöglichen, die Sie für DNS-Abfragen in Ihrem Netzwerk verwenden. Port 53 wird im obigen Beispiel gezeigt, da es sich um den gängigsten DNS-Port handelt, Ihr Netzwerk jedoch möglicherweise andere Ports verwendet. Durch Eingangsregeln können alle Ports Antworten von Ihren DNS-Servern aufnehmen.

Resolver-Endpunkt

Bei Clients, die einen eingehenden Resolverendpunkt verwenden, wird die Kapazität der elastic network interface beeinträchtigt, wenn Sie über 40.000 eindeutige IP-Adress- und Portkombinationen verfügen, die den DNS-Datenverkehr generieren.

Hohe Verfügbarkeit für Resolver-Endpunkt

Wenn Sie Ihre eingehenden VPC-Resolver-Endpunkte erstellen, erfordert Route 53, dass Sie mindestens zwei IP-Adressen erstellen, an die die DNS-Resolver in Ihrem Netzwerk Anfragen weiterleiten. Sie sollten zu Redundanzzwecken auch IP-Adressen in mindestens zwei Availability Zones angeben.

Wenn Sie benötigen, dass immer mehr als ein Endpunkt der elastic network interface verfügbar ist, empfehlen wir, mindestens eine weitere Netzwerkschnittstelle zu erstellen, als Sie benötigen, um sicherzustellen, dass zusätzliche Kapazitäten für die Handhabung möglicher Überspannungen verfügbar sind. Die zusätzliche Netzwerkschnittstelle stellt auch die Verfügbarkeit während des Servicebetriebs wie Wartung oder Upgrades sicher.

Weitere Informationen finden Sie in diesem ausführlichen Blogartikel: So erreichen Sie DNS-Hochverfügbarkeit mit Resolver-Endpunkten und. Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben

Gehen Sie zur DNS-Zone

Ein DNS-Zonenangriff versucht, alle Inhalte von DNSSEC-signierten DNS-Zonen abzurufen. Wenn das VPC-Resolver-Team ein Datenverkehrsmuster erkennt, das mit denen übereinstimmt, die beim Durchlaufen von DNS-Zonen auf Ihrem Endpunkt generiert wurden, drosselt das Service-Team den Verkehr auf Ihrem Endpunkt. Als Konsequenz können Sie einen hohen Prozentsatz Ihrer DNS-Abfragen beobachten, der Timeout ist.

Wenn Sie eine verringerte Kapazität auf Ihren Endpunkten feststellen und glauben, dass der Endpunkt irrtümlich gedrosselt wurde, gehen Sie zu home#/, um einen Support-Fall zu https://console.aws.amazon.com/support/ erstellen.

Bewährte Methoden für Amazon Route 53 Zustandsprüfungen

Eine effektive Konfiguration der Systemdiagnose ist für die Aufrechterhaltung einer hochverfügbaren und ausfallsicheren Infrastruktur unerlässlich. Im Folgenden finden Sie einige bewährte Methoden, die Sie bei der Einrichtung und Verwaltung von Amazon Route 53-Zustandsprüfungen berücksichtigen sollten:

1. Verwenden Sie elastische IP-Adressen für Endpunkte zur Zustandsprüfung:
   - Verwenden Sie elastische IP-Adressen für Ihre Health Check-Endpunkte, um eine konsistente Überwachung zu gewährleisten.
   - Wenn Sie eine EC2 Amazon-Instance nicht mehr verwenden, denken Sie daran, alle zugehörigen Zustandsprüfungen zu löschen, um potenzielle Sicherheitsrisiken oder Datenkompromittierungen zu vermeiden.

   Weitere Informationen finden Sie unterWerte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen.
2. Konfigurieren Sie die entsprechenden Intervalle für Integritätsprüfungen:
   - Legen Sie Intervalle für Integritätsprüfungen auf der Grundlage der Anforderungen Ihrer Anwendung und der Wichtigkeit der überwachten Ressourcen fest.
   - Kürzere Intervalle ermöglichen eine schnellere Fehlererkennung, können jedoch die Kosten für Route 53 erhöhen und Ihre Ressourcen belasten.

- Längere Intervalle reduzieren die Kosten und die Ressourcenbelastung, können jedoch die Fehlererkennung verzögern.

Weitere Informationen finden Sie unterErweiterte Konfiguration (nur "Monitor an endpoint").

3. Implementieren Sie Alarmbenachrichtigungen:
   - Konfigurieren Sie Amazon so CloudWatchalarms , dass es Benachrichtigungen erhält, wenn Zustandsprüfungen fehlschlagen oder wiederhergestellt werden.
   - Legen Sie je nach den Anforderungen Ihrer Anwendung und dem erwarteten Verhalten Ihrer Ressourcen geeignete Alarmschwellenwerte fest.
   - Integrieren Sie Benachrichtigungen in Ihre Überwachungs- und Reaktionsprozesse.

   Weitere Informationen finden Sie unterÜberwachung von Zustandsprüfungen mit CloudWatch.
4. Nutzen Sie die Regionen mit dem Gesundheitscheck strategisch:
   - Wählen Sie die Health Check-Regionen auf der Grundlage der geografischen Verteilung Ihrer Benutzer und Ressourcen aus.
   - Erwägen Sie die Verwendung mehrerer Regionen mit Gesundheitschecks für wichtige Ressourcen, um die Zuverlässigkeit zu erhöhen und die Auswirkungen regionaler Ausfälle zu verringern.
5. Überwachen Sie die Protokolle und Metriken der Gesundheitschecks:
   - Überprüfen Sie regelmäßig die Protokolle und CloudWatch Metriken der Route 53-Zustandsprüfungen, um potenzielle Probleme oder Leistungsengpässe zu identifizieren
   - Analysieren Sie die Gründe für Fehlschläge bei der Zustandsprüfung und ergreifen Sie geeignete Maßnahmen, um die zugrunde liegenden Probleme zu lösen.
6. Implementieren Sie Failover- und Failback-Strategien:
   - Nutzen Sie die Failover-Routing-Richtlinien von Route 53, um den Datenverkehr bei Ausfällen automatisch an fehlerfreie Ressourcen weiterzuleiten.
   - Planen und testen Sie Failover- und Failback-Prozesse, um einen reibungslosen Übergang bei Ausfällen und bei der Wiederherstellung sicherzustellen.

   Weitere Informationen finden Sie unter. Konfigurieren von DNS Failover
7. Überprüfen und aktualisieren Sie regelmäßig die Gesundheitschecks:
   - Aktualisieren Sie die Endpunkte, Intervalle und Alarmschwellenwerte für Integritätsprüfungen nach Bedarf, um eine optimale Überwachung und Leistung aufrechtzuerhalten.

Wenn Sie diese bewährten Methoden befolgen, können Sie Amazon Route 53 Health Checks effektiv nutzen, um den Zustand und die Verfügbarkeit Ihrer Ressourcen zu überwachen und so eine zuverlässige und leistungsstarke Infrastruktur für Ihre Anwendungen und Services zu gewährleisten.

Kontingente

Amazon Route 53-API-Anfragen und Entitäten unterliegen den folgenden Kontingenten (früher als „Limits“ bezeichnet).

Themen

Verwenden von Service Quotas zum Anzeigen und Verwalten von Kontingenten

Sie können Service Service Quotas verwenden, um Kontingente anzuzeigen und Kontingenterhöhungen für viele AWS -Services anzufordern. Weitere Informationen zu diesem Service finden Sie im Benutzerhandbuch für Service Quotas. (Sie können derzeit Service Quotas verwenden, um Domänen, Route 53- und Route 53 VPC Resolver-Kontingente anzuzeigen und zu verwalten.)

> **Note**
>
> Um Kontingente anzuzeigen und höhere Kontingente für Route 53 anzufordern, müssen Sie die Region in USA Ost (Nord-Virginia) ändern. Um Kontingente anzuzeigen und höhere Kontingente für VPC Resolver anzufordern, wechseln Sie zur entsprechenden Region.

Kontingente für Entitäten

Amazon Route 53-Entitäten unterliegen den folgenden Kontingenten.

Informationen zum Abrufen aktueller Kontingente (früher als „Limits“ bezeichnet) finden Sie unter den folgenden Route 53 Aktionen:

- GetAccountLimit— Ruft Kontingente für Integritätsprüfungen, gehostete Zonen, wiederverwendbare Delegierungssätze, Verkehrsflussrichtlinien und Datenverkehrsflussrichtlinien-Datensätze ab

- GetHostedZoneLimit— Ruft Kontingente für Datensätze in einer gehosteten Zone und bei Amazon ab VPCs , die Sie einer privaten gehosteten Zone zuordnen können
- GetReusableDelegationSetLimit— Ruft das Kontingent für die Anzahl von Hosting-Zonen ab, die Sie einem wiederverwendbaren Delegierungssatz zuordnen können

Themen

Kontingente für Domänen

Entität	Kontingent
Domains	20* pro Konto AWS Request a higher quotaf (Höheres Kontingent anfordern).

*Das Limit für Neukunden beträgt ab März 2021 20.

Wenn Sie ein bestehendes Konto haben und Ihr Standardlimit jetzt 50 beträgt, bleibt es bei 50.

Kontingente für gehostete Zonen

Entität	Kontingent

Entität	Kontingent
Gehostete Zonen	Anfängliches Kontingent von 500 pro AWS Konto, aber Sie können bei Bedarf ein höheres Kontingent beantragen. Request a higher quota (Höheres Kontingent anfordern).
Gehostete Zonen, die den gleichen wiederverwendbaren Delegationssatz verwenden können	100 Request a higher quota (Höheres Kontingent anfordern).
Amazon VPCs , das Sie einer privaten gehosteten Zone pro gehosteter Zone zuordnen können	300 Wenn Sie mehr als 300 Verknüpfungen wünschen, empfehlen wir Ihnen, Route 53 53-Profile zu verwenden. Weitere Informationen finden Sie unter Was sind Amazon Route 53 53-Profile?.
Private gehostete Zone, denen Sie eine VPC zuordnen können	Kein Kontingent *
Autorisierungen, die Sie erstellen können, um VPCs die von einem Konto erstellten Berechtigungen einer Hosting-Zone zuzuordnen, die von einem anderen Konto erstellt wurde	1000
Die Anzahl der Schlüsselsignierungsschlüssel (KSK), die pro gehosteter Zone erstellt werden können	2

* Sie können eine VPC mit einer oder allen privaten Hosting-Zonen verknüpfen, die Sie über Ihre AWS Konten kontrollieren. Nehmen wir zum Beispiel an, Sie haben drei AWS Konten und alle drei

haben das Standardkontingent von 500 gehosteten Zonen. Wenn Sie 500 private gehostete Zonen für alle drei Konten erstellen, können Sie allen 1.500 privat gehosteten Zonen eine VPC zuordnen.

Kontingente für Datensätze

Entität	Kontingent
Datensätze	10.000 pro gehostete Zone Request a higher quota (Höheres Kontingent anfordern). Für ein Kontingent von mehr als 10.000 Datensätzen in einer gehosteten Zone fällt eine zusätzliche Gebühr an. Weitere Informationen finden Sie unter Amazon Route 53 – Preise.
Datensätze in einer Datensatzgruppe	400 pro Datensatzgruppe
Geolocation, Latenz, mehrwertige Antwort, gewichtete und IP-basierte Datensätze	100 Datensätze mit demselben Namen und Typ
Geoproximity-Datensätze	30 Datensätze mit demselben Namen und Typ
CIDR-Sammlungen	5 pro. AWS-Konto Request a higher quotaf (Höheres Kontingent anfordern).
CIDR-Blöcke	1 000 pro CIDR-Sammlung. Request a higher quotaf (Höheres Kontingent anfordern).

Kontingente auf Route 53 VPC Resolver

Dieser Abschnitt enthält alle Route 53 VPC Resolver-Kontingente.

Kontingente auf Route 53 VPC Resolver

Gehen Sie wie folgt vor, um die Kontingente für Route 53 VPC Resolver zu erhöhen.

So erhöhen Sie das Kontingent für Resolver

1. Öffnen Sie die Service Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas.
2. Wechseln Sie zu der Region, in der Sie das Limit erhöhen möchten.
3. Wählen Sie den Route 53 VPC Resolver-Kontingentnamen aus, den Sie erhöhen möchten.
4. SelectKontingenterhöhung anfordern, geben Sie den Kontingentwert ein, und wählen Sie dannAnfrageaus.

Kontingente auf Route 53 53-VPC-Resolver-Endpunkten

Entität	Kontingent
Endpunkte pro Region AWS	4 pro Konto AWS Request a higher quota (Höheres Kontingent anfordern).
IP-Adressen pro Endpunkt	6 Request a higher quota (Höheres Kontingent anfordern).
IP-Adressen pro Regel	6
Regeln pro AWS Region	1000 pro AWS Konto Request a higher quotaf (Höheres Kontingent anfordern).
Assoziationen zwischen Regeln und VPCs pro AWS Region	2000 pro AWS Konto Request a higher quotaf (Höheres Kontingent anfordern).

Entität	Kontingent
UDP-Abfragen pro Sekunde pro IP-Adresse in einem Endpunkt	10.000*

* Jede IP-Adresse in einem Endpunkt kann bis zu 10.000 UDP-DNS-Abfragen pro Sekunde (QPS) verarbeiten. Die Anzahl der DNS-QPS variiert je nach Abfragetyp, Größe der Antwort, Integrität der Zielnamenserver, Abfragereaktionszeiten,Round-Trip-Latenz, und das verwendete Protokoll. Beispielsweise können Abfragen an einen Zielnamenserver, der langsam reagiert, die Kapazität der Netzwerkschnittstelle erheblich verringern. Darüber hinaus generiert Route 53 Resolver redundante ausgehende Abfragen für jede empfangene DNS-Anforderung, um eine hohe Verfügbarkeit sicherzustellen. Infolgedessen stimmt der QPS für jede ausgehende Netzwerkschnittstelle nicht mit dem QPS überein, der an den Route 53 VPC Resolver gesendet wurde. Verwenden Sie CloudWatch Metriken, um zu messen, wie viele Anfragen an jede Netzwerkschnittstelle gesendet werden. Weitere Informationen finden Sie unter Metriken für Route 53 VPC Resolver-IP-Adressen. Wenn die maximale Abfragerate 50% der Kapazität einer Netzwerkschnittstelle im Endpunkt überschreitet, können Sie weitere Netzwerkschnittstellen hinzufügen, um die Endpunktkapazität zu erhöhen.

Verbindungen, die über Anwendungen wie Network Load Balancer und AWS Lambda (eine vollständige Liste finden Sie unter Automatisch verfolgte Verbindungen) hergestellt werden, werden automatisch nachverfolgt, auch wenn die Sicherheitsgruppenkonfiguration ansonsten kein Tracking erfordert.

Wenn die Verbindungsverfolgung entweder mithilfe restriktiver Sicherheitsgruppenregeln erzwungen wird oder Abfragen über den Network Load Balancer weitergeleitet werden, kann die maximale Gesamtzahl der Abfragen pro Sekunde pro IP-Adresse für einen eingehenden Endpunkt bis zu 1500 betragen.

Kontingente für Route 53 VPC Resolver-Abfrageprotokolle

Entität	Kontingent
Log-Konfigurationen pro Region abfragen AWS	20 Request a higher quotaf (Höheres Kontingent anfordern).

Entität	Kontingent
Abfrageprotokollkonfiguration VPC Zuordnungen pro AWS -Region	100 * Request a higher quotaf (Höheres Kontingent anfordern).
Abfragen von VPC-Zuordnungen der Protokollkonfiguration pro Konto pro AWS Region (einschließlich langer Abfragekonfigurationen, die über RAM gemeinsam genutzt werden) für das Konto, für das die Konfiguration gemeinsam genutzt wurde.	100 Request a higher quota (Höheres Kontingent anfordern).

* Dies ist ein regionales Limit, das kumulativ für alle VPC Resolver-Abfrageprotokollkonfigurationen innerhalb einer einzelnen Region gilt. Das Erstellen zusätzlicher Abfrageprotokollkonfigurationen in derselben Region bietet keine zusätzliche VPC-Zuordnungskapazität.

Kontingente auf der Resolver DNS Firewall

Entität	Kontingent
Anzahl der Regelgruppen, die einer VPC für ein einzelnes Konto pro AWS -Region	5
Anzahl der DNS-Firewall-Domains in einer einzigen Amazon S3 S3-Datei für ein einzelnes Konto pro AWS Region	250 000 Request a higher quotaf (Höheres Kontingent anfordern).
Anzahl der DNS-Firewall-Regel gruppen für ein einzelnes Konto pro AWS Region	1.000 Request a higher quota (Höheres Kontingent anfordern).
	100

Entität	Kontingent
Anzahl der Regeln innerhalb einer Regelgruppe für ein einzelnes Konto pro AWS Region	Request a higher quota (Höheres Kontingent anfordern).
Anzahl der Domainlisten für ein einzelnes Konto pro AWS Region	1000 Request a higher quota (Höheres Kontingent anfordern).
Die maximale Anzahl von Domains, die Sie für alle Domainlisten für ein einzelnes Konto pro AWS Region angeben können	100 000 Request a higher quota (Höheres Kontingent anfordern).

Kontingente für Resolver auf Outpost

Entität	Kontingent
Instance-Limit für Resolver auf Outpost	6 (mindestens 4 erforderlich)

Instanztypen für Resolver auf Outpost und Anzahl der DNS-Abfragen pro Sekunde, die jeder Instanztyp verarbeiten kann:

Instance-Typ	Abfragen pro Sekunde
c5.large	Bis zu 7 000
c5.xlarge	Bis zu 12 000
c5.2xlarge	Bis zu 24 000
c5.4xlarge	Bis zu 56 000

Instance-Typ	Abfragen pro Sekunde
c5d.large	Bis zu 7 000
c5d.xlarge	Bis zu 12 000
c5d.2xlarge	Bis zu 24 000
c5d.4xlarge	Bis zu 56 000
m5.large	Bis zu 7 000
m5.xlarge	Bis zu 12 000
m5.2xlarge	Bis zu 24 000
m5.4xlarge	Bis zu 56 000
m5d.large	Bis zu 7 000
m5d.xlarge	Bis zu 12 000
m5d.2xlarge	Bis zu 24 000
m5d.4xlarge	Bis zu 56 000
r5.large	Bis zu 7 000
r5.xlarge	Bis zu 12 000

Instance-Typ	Abfragen pro Sekunde
r5.2xlarge	Bis zu 24 000
r5.4xlarge	Bis zu 56 000
r5d.large	Bis zu 7 000
r5d.xlarge	Bis zu 12 000
r5d.2xlarge	Bis zu 24 000
r5d.4xlarge	Bis zu 56 000

Instanztypen für Resolver auf Outpost-Endpunkten und Anzahl der DNS-Abfragen pro Sekunde, die jeder Instance-Typ verarbeiten kann:

Instance-Typ	Abfragen pro Sekunde
c5.large	Bis zu 5 000
c5.xlarge	Bis zu 10 000*
c5.2xlarge	Bis zu 18 000
c5.4xlarge	Bis zu 30 000
c5d.large	Bis zu 5 000
c5d.xlarge	Bis zu 10 000*
c5d.2xlarge	Bis zu 18 000

Instance-Typ	Abfragen pro Sekunde
c5d.4xlarge	Bis zu 30 000
m5.large	Bis zu 5 000
m5.xlarge	Bis zu 10 000*
m5.2xlarge	Bis zu 18 000
m5.4xlarge	Bis zu 30 000
m5d.large	Bis zu 5 000
m5d.xlarge	Bis zu 10 000*
m5d.2xlarge	Bis zu 18 000
m5d.4xlarge	Bis zu 30 000
r5.large	Bis zu 5 000
r5.xlarge	Bis zu 10 000*
r5.2xlarge	Bis zu 18 000
r5.4xlarge	Bis zu 30 000
r5d.large	Bis zu 5 000

Instance-Typ	Abfragen pro Sekunde
r5d.xlarge	Bis zu 10 000*
r5d.2xlarge	Bis zu 18 000
r5d.4xlarge	Bis zu 30 000

Kontingente für Zustandsprüfungen

Entität	Kontingent
Health checks (Zustandsprüfungen)	200 aktive Zustandsprüfungen pro Konto AWS Request a higher quota (Höheres Kontingent anfordern).
Untergeordnete Zustandsprüfungen, die eine berechnete Zustandsprüfung überwachen kann	255
Maximale Gesamtlänge der Header in der Antwort auf eine Zustandsprüfungsanforderung	16.384 Bytes (16K)

Kontingente für Abfrageprotokollkonfigurationen

Entität	Kontingent
Abfrageprotokollkonfigurationen	1 pro gehostete Zone

Kontingente für Datenflussrichtlinien und Richtliniendatensätze

Entität	Kontingent
Datenverkehrsrichtlinien Weitere Informationen zum Route 53-Datenfluss finden Sie unter Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr.	50 pro AWS Konto Request a higher quota (Höheres Kontingent anfordern).
Versionen der Datenverkehrsrichtlinie	1.000 pro Datenverkehrsrichtlinie
Datensätze zur Verkehrsrichtlinie (in der Route 53-API als „Richtlinieninstanzen“ bezeichnet AWS SDKs, AWS Command Line Interface, und AWS Tools for Windows PowerShell)	5 pro AWS Konto Request a higher quota (Höheres Kontingent anfordern).

Kontingente für wiederverwendbare Delegationssätze

Entität	Kontingent
Wiederverwendbare Delegationssätze	100 pro AWS Konto Request a higher quotaf (Höheres Kontingent anfordern).

Kontingente für Route 53 53-Profile

Entität	Kontingent
	5

Entität	Kontingent
Anzahl der Route 53 53-Profile pro AWS-Konto Region	Request a higher quotaf (Höheres Kontingent anfordern).
Anzahl davon VPCs , die einem Profil zugeordnet werden können	1000 Request a higher quota (Höheres Kontingent anfordern).
Anzahl der DNS-Firewall-Regel gruppen pro Profil	5
Anzahl der Resolver-Regeln pro Profil	1000 Request a higher quota (Höheres Kontingent anfordern).
Anzahl der privat gehosteten Zonen pro Profil	1.000 Request a higher quota (Höheres Kontingent anfordern).
Anzahl der VPC-Resolver-Abfra geprotokollierungskonfigurationen pro Profil	2

Höchstwerte bei API-Anfragen

Amazon Route 53-API-Anforderungen unterliegen den folgenden Kontingenten.

Themen

- Anzahl der Elemente und Zeichen in ChangeResourceRecordSets-Anforderungen
- Häufigkeit der Amazon Route 53 API-Anforderungen
- Häufigkeit von Route 53 VPC Resolver API-Anfragen

Anzahl der Elemente und Zeichen in **`ChangeResourceRecordSets`**-Anforderungen

`ResourceRecord`-Elemente

Eine Anforderung darf nicht mehr als 1.000 `ResourceRecord`-Elemente enthalten (einschließlich Alias-Datensätzen). Wenn der Wert des `Action`-Elements `UPSERT` ist, wird jedes `ResourceRecord`-Element zweimal gezählt.

Maximale Anzahl von Zeichen

Die Summe der Anzahl der Zeichen (einschließlich Leerzeichen) in allen `Value`-Elementen in einer Anforderung darf als 32.000 Zeichen nicht überschreiten. Wenn der Wert des `Action`-Elements `UPSERT` ist, wird jedes Zeichen in einem `Value`-Element zweimal gezählt.

Häufigkeit der Amazon Route 53 API-Anforderungen

Alle Amazon Route 53-API-Anfragen

Für Amazon Route 53 APIs fünf Anfragen pro Sekunde pro AWS Konto. Wenn Sie mehr als fünf Anforderungen pro Sekunde senden, gibt Amazon Route 53 einen HTTP 400-Fehler zurück (`Bad request`). Der Antwort-Header umfasst außerdem ein `Code`-Element mit dem Wert `Throttling` und ein `Message`-Element mit dem Wert `Rate exceeded`.

> **Note**
>
> Wenn Ihre Anwendung diesen Grenzwert überschreitet, wird empfohlen, exponentielles Backoff für Wiederholungen zu implementieren. Weitere Informationen finden Sie unter Wiederholversuche bei Fehlern und exponentielles Backoff in AWS im Allgemeine Amazon Web Services-Referenz.

`ChangeResourceRecordSets`-Anforderungen

Wenn Route 53 eine Anforderung nicht verarbeiten kann, bevor die nächste Anforderung eintrifft, werden nachfolgende Anforderungen für dieselbe gehostete Zone abgelehnt und ein HTTP 400-Fehler (`Bad request`) zurückgegeben. Der Antwort-Header umfasst außerdem ein `Code`-Element mit dem Wert `PriorRequestNotComplete` und ein `Message`-Element mit dem Wert

`The request was rejected because Route 53 was still processing a prior request.`

`CreateHealthCheck`-Anforderungen

Sie können alle 2 Sekunden eine `CreateHealthCheck` Anfrage einreichen AWS-Konto.

Häufigkeit von Route 53 VPC Resolver API-Anfragen

Alle Anforderungen

Fünf Anfragen pro Sekunde pro AWS Konto pro Region. Wenn Sie in einer Region mehr als fünf Anfragen pro Sekunde einreichen, gibt VPC Resolver einen HTTP 400-Fehler () `Bad request` zurück. Der Antwort-Header umfasst außerdem ein `Code`-Element mit dem Wert `Throttling` und ein `Message`-Element mit dem Wert `Rate exceeded`.

> **Note**
>
> Wenn Ihre Anwendung diesen Grenzwert überschreitet, wird empfohlen, exponentielles Backoff für Wiederholungen zu implementieren. Weitere Informationen finden Sie unter Wiederholversuche bei Fehlern und exponentielles Backoff in AWS im Allgemeine Amazon Web Services-Referenz.

Ähnliche Informationen

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

Themen

- AWS Ressourcen
- Drittanbieter-Tools und Bibliotheken
- Grafische Benutzeroberflächen

AWS Ressourcen

Zu Amazon Web Services sind verschiedene hilfreiche Anleitungen, Foren und andere Ressourcen verfügbar.

- Amazon-Route-53-API-Referenz – Ein Referenzhandbuch, das den Speicherort des Schemas, eine umfassende Beschreibung der API-Aktionen, Parameter und Datentypen sowie eine Liste von Fehlern, die der Service zurückgibt, enthält.
- AWS::Route53::RecordSet Geben Sie das AWS CloudFormation Benutzerhandbuch ein — Eine Eigenschaft für die Verwendung von Amazon Route 53, mit der CloudFormation Sie benutzerdefinierte DNS-Namen für Ihre CloudFormation Stacks erstellen können.
- -Diskussionsforen – Ein Community-basiertes für Entwickler, um über technische Fragen zu Route 53 zu diskutieren.
- AWS Support Center — Diese Website enthält Informationen zu Ihren aktuellen Supportfällen und Ergebnissen von AWS Trusted Advisor und Zustandsprüfungen sowie Links zu Diskussionsforen, technischen Informationen FAQs, dem Service Health Dashboard und Informationen zu AWS Supportplänen.
- AWS Premium-Support-Informationen — Die wichtigste Webseite mit Informationen zu AWS Premium Support, einem Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen auf AWS Infrastructure Services unterstützt.
- Kontakt – Links zu Informationen zu Ihrer Abrechnung. Technische Fragen stellen Sie bitte in den Diskussionsforen oder über die Support-Links.
- Route-53-Produktinformationen – Die Hauptwebsite für Informationen zu Route 53 mit Funktionen, Preisen und mehr.

- Kurse und Workshops — Links zu rollen- und Spezialkursen sowie zu Übungen zum Selbststudium, mit denen Sie Ihre AWS Fähigkeiten verbessern und praktische Erfahrungen sammeln können.
- AWS Developer Center — Erkunden Sie Tutorials, laden Sie Tools herunter und erfahren Sie mehr über Veranstaltungen für Entwickler. AWS
- AWS Entwicklertools — Links zu Entwicklertools SDKs, IDE-Toolkits und Befehlszeilentools für die Entwicklung und Verwaltung von AWS Anwendungen.
- Ressourcencenter für die ersten Schritte — Erfahren Sie AWS-Konto, wie Sie Ihre erste Anwendung einrichten, der AWS Community beitreten und sie starten.
- Praktische Tutorials — Folgen Sie den step-by-step Tutorials, um Ihre erste Anwendung zu starten. AWS
- AWS Whitepapers — Links zu einer umfassenden Liste von technischen AWS Whitepapers zu Themen wie Architektur, Sicherheit und Wirtschaft, die von Solutions Architects oder anderen technischen Experten verfasst wurden. AWS
- AWS Support Center — Die zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer Fälle. AWS Support Enthält auch Links zu anderen hilfreichen Ressourcen wie Foren, technischen FAQs Informationen, Servicestatus und AWS Trusted Advisor.
- Support— Die wichtigste Webseite mit Informationen über Support einen Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen in der Cloud unterstützt.
- Kontakt – Zentraler Kontaktpunkt für Fragen zu AWS -Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- AWS Nutzungsbedingungen der Website — Detaillierte Informationen zu unseren Urheberrechten und Marken, zu Ihrem Konto, Ihrer Lizenz und Ihrem Zugriff auf die Website sowie zu anderen Themen.

Drittanbieter-Tools und Bibliotheken

Zusätzlich zu den AWS Ressourcen finden Sie eine Vielzahl von Tools und Bibliotheken von Drittanbietern, die mit Amazon Route 53 funktionieren.

- AmazonRoute53 AppsScript (über Webos-Goodies)

  Google-Tabellenverwaltung von Amazon Route 53.
- AWS Komponente für .NET (via) SprightlySoft

SprightlySoft .NET-Komponente für Amazon Web Services mit Unterstützung für REST-Operationen und Route 53.

- Boto API-Download (über github)

  Boto Python-Schnittstelle für Amazon Web Services.

- cli53 (über github)

  Befehlszeilenschnittstelle für Route 53.

- Dasein Cloud-API

  Java-basierte API.

- R53.py (über github)

  Verwaltet eine kanonische Version Ihrer DNS-Konfigurationen unter Quellüberwachung und berechnet die Änderungen, die mindestens erforderlich sind, um eine Konfiguration zu ändern.

- route53d

  DNS-Frontend zu Route-53-API (ermöglicht inkrementelle Zonenübertragung (IXFR)).

- Route53Manager (über github)

  Webbasierte Schnittstelle.

- Ruby Fog (über github)

  Ruby Cloud Services-Bibliothek.

- WebService: :Amazon: :Route53 (über CPAN)

  Perl-Schnittstelle zur Amazon-Route-53-API.

Grafische Benutzeroberflächen

Die folgenden Drittanbieter-Tools bieten grafische Benutzeroberflächen (GUIs) für die Arbeit mit Amazon Route 53:

- R53 Fox
- Ylastic

Dokumentverlauf

In der folgenden Auflistung sind wichtige Änderungen in jeder Version dieser Dokumentation zu Route 53 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Themen

Veröffentlichungen 2025

15. Dezember 2025

Es wurden detaillierte CloudWatch Metriken für Route 53 Resolver-Endpunkte hinzugefügt. Die neuen Metriken bieten erweiterte Überwachungsfunktionen auf den Ebenen Resolver Network Interface und Target Name Server, darunter die P90-Antwortlatenz von DNS-Abfragen, die Verfolgung der Antwortstatus SERVFAIL, NXDOMAIN, REFUSED und FORMERR sowie die

Verfügbarkeitsüberwachung der Ziel-Nameserver für ausgehende Resolver-Endpunkte. Weitere Informationen finden Sie unter CloudWatch Detaillierte Metriken für Route 53 VPC Resolver.

26. Juni 2025

`ResolverEndpointCapacityStatus`AWS/Route53ResolverZum Namespace hinzugefügt. Weitere Informationen finden Sie unter Metriken für Route 53 VPC Resolver-Endpunkte.

25. Juni 2025

Amazon Route 53 unterstützt jetzt Aliaseinträge für benutzerdefinierte Domänenendpunkte des VPC Lattice-Dienstes. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an den Domänenendpunkt des Amazon VPC Lattice-Dienstes.

24. Juni 2025

Sie können jetzt eingehende und ausgehende Delegierung mit VPC Resolver verwenden. Weitere Informationen finden Sie unter Wie DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Resolver-Endpunkte weiterleiten.

01. Juni 2025

Es wurden Berechtigungen für `cloudwatch:GetMetricDatatag:GetResources`,`es:ListDomainNames`, `es:DescribeDomainscloudfront:GetDistributionTenantByDomain`, `cloudfront:GetConnectionGroup` und hinzugefügt`lightsail:GetContainerServices`. Mit diesen Berechtigungen können Sie bis zu 500 CloudWatch Health Check-Metriken und bis zu 100 Namen von Zustandsprüfungen abrufen, die Domain-Konfiguration für die angegebenen Amazon OpenSearch Service-Domains abrufen und die Namen aller Amazon OpenSearch Service-Domains auflisten, die dem aktuellen Benutzer in der aktiven Region gehören, die CloudFront Multi-Tenant-Distributionen abrufen und die Lightsail-Container-Services abrufen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonRoute 53 FullAccess.

28. April 2025

Sie können jetzt VPC-Schnittstellen-Endpunkte Route 53 53-Profilen zuordnen. Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte einem Route 53 53-Profil zuordnen.

28. April 2025

Sie können jetzt einem CloudFront Verteilungsmandanten einen Aliaseintrag hinzufügen. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

27. Februar 2025

Der Route 53-Leitfaden wurde mit der neuen Konsolenoberfläche für Traffic Flow aktualisiert. Weitere Informationen erhalten Sie unter Erstellen und Verwalten von Datenverkehrsrichtlinien und Erstellen und Verwalten von Richtliniendatensätzen.

14. Januar 2025

Amazon Route 53 unterstützt jetzt Alias-Datensätze für benutzerdefinierte OpenSearch Service-Domain-Endpunkte. Weitere Informationen finden Sie unter Weiterleitung des Datenverkehrs an den Amazon OpenSearch Service-Domänenendpunkt.

13. Januar 2025

Die Ergebnisse der Resolver-DNS-Firewall wurden dem Security Hub CSPM hinzugefügt. Weitere Informationen finden Sie unter Ergebnisse von der Resolver DNS Firewall an Security Hub CSPM senden.

Veröffentlichungen von 2024

15. November 2024

Resolver DNS Firewall Advanced wurde hinzugefügt, ein neuer Funktionsumfang der Resolver DNS Firewall, mit dem Sie DNS-Verkehr identifizieren und blockieren können, der mit fortgeschrittenen DNS-Bedrohungen wie DNS-Tunneling, Domain Generation Algorithm (DGA) und Dictionary DGA-basierten Bedrohungen verbunden ist. Weitere Informationen finden Sie unter Resolver DNS Firewall Advanced.

29. Oktober 2024

Unterstützung für die DNS-Eintragstypen HTTPS, SSHFP, SVCB und TLSA wurde hinzugefügt. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

3. Oktober 2024

Unterstützung für Service Name Indication (SNI) für ausgehende DoH-Resolver-Endpunkte hinzugefügt. Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Regeln angeben.

3. September 2024

Sie können jetzt die `route53:VPCs` Richtlinienbedingung verwenden, um detaillierten Zugriff auf die Verwaltung von Zuordnungen zu gehosteten Zonen zu gewähren. VPCs Weitere

Informationen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

27. August 2024

`AmazonRoute53ProfilesFullAccess`Berechtigungen für `GetProfilePolicy` und hinzugefügt`PutProfilePolicy`. Dies sind IAM-Aktionen, die nur für Berechtigungen gelten. Wenn einem IAM-Prinzipal diese Berechtigungen nicht erteilt wurden, tritt beim Versuch, das Profil über den AWS RAM Dienst freizugeben, ein Fehler auf. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: 53 AmazonRoute ProfilesFullAccess.

27. August 2024

`AmazonRoute53ProfilesReadOnlyAccess`Erlaubnis für hinzugefügt`GetProfilePolicy`. Dies ist eine IAM-Aktion, für die nur Berechtigungen erforderlich sind. Wenn einem IAM-Prinzipal diese Berechtigung nicht erteilt wurde, tritt beim Versuch, über den Dienst auf die Richtlinie des Profils zuzugreifen, ein Fehler auf. AWS RAM Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonRoute 53 ProfilesReadOnlyAccess.

5. August 2024

Es wurde eine Anweisungs-ID (Sid) hinzugefügt, um die verwaltete Richtlinie `AmazonRoute53ResolverFullAccess` eindeutig zu identifizieren. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonRoute 53 ResolverFullAccess.

5. August 2024

Es wurde eine Anweisungs-ID (Sid) hinzugefügt, um die verwaltete Richtlinie eindeutig zu identifizieren`AmazonRoute53ResolverReadOnlyAccess`. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonRoute 53 ResolverReadOnlyAccess.

18. Juli 2024

Der gesamte Route 53-Leitfaden wurde mit der neuen Konsolenoberfläche für Integritätsprüfungen aktualisiert. Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

30. April 2024

Sie können jetzt entscheiden, ob eine DNS-Firewallregel die DNS-Umleitungskette entweder überprüft (Standard) oder ihr vertraut. Weitere Informationen erhalten Sie unter Komponenten und Einstellungen der Resolver DNS-Firewall und Regeleinstellungen in der DNS-Firewall.

22. April 2024

Sie können jetzt Route 53 53-Profile verwenden, um DNS-spezifische Konfigurationen mit vielen VPCs und mit AWS Konten zu teilen. Weitere Informationen finden Sie unter Was sind Amazon Route 53 53-Profile?.

22. April 2024

Die verwalteten Richtlinien `AmazonRoute53ProfilesReadOnlyAccess` und `AmazonRoute53ProfilesFullAccess` die Gewährung von schreibgeschütztem und vollständigem Zugriff auf Amazon Route 53 53-Profile wurden hinzugefügt. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon Route 53.

5. Februar 2024

Sie können Amazon jetzt EventBridge für Echtzeitwarnungen mit der DNS-Firewall verwenden. Weitere Informationen finden Sie unter Verwaltung von Resolver-DNS-Firewall-Ereignissen mit Amazon EventBridge.

9. Januar 2024

Sie können jetzt den DNS-Abfragetyp als optionalen Wert für die DNS-Firewall-Regel verwenden, um die Antwort der Regel für einen bestimmten DNS-Abfragetyp zu unterscheiden. Weitere Informationen erhalten Sie unter Komponenten und Einstellungen der Resolver DNS-Firewall und Regeleinstellungen in der DNS-Firewall.

9. Januar 2024

Sie können jetzt den Assistenten „Datensatz schnell erstellen“ oder „Datensatz erstellen“ verwenden, um Geoproximity-Routing-Datensätze zu erstellen. Weitere Informationen finden Sie unter Geoproximity-Routing, Spezifische Werte für Geoproximitätsdatensätze und Spezifische Werte für Geoproximitäts-Aliasdatensätze.

Veröffentlichungen 2023

20. Dezember 2023

Sie können jetzt DNS über HTTPS mit Resolver-Endpunkten verwenden. Weitere Informationen finden Sie unter Auswählen von Protokollen für die Endpunkte.

20. Juli 2023

Amazon Route 53 on Outposts ist jetzt in AWS Outposts Racks verfügbar. Es enthält einen VPC-Resolver, der alle DNS-Abfragen zwischenspeichert, die von der stammen. AWS Outposts Sie können auch Hybridkonnektivität zwischen einem Outpost und einem On-Premises-DNS-Resolver einrichten, wenn Sie ein- und ausgehende Endpunkte bereitstellen. Weitere Informationen finden Sie unter Was ist Amazon Route 53 auf Outposts?.

19. Juli 2023

Sie können jetzt nach der Aktivierung von Local Zones das Routing auf Grundlage der geografischen Nähe verwenden (nur Datenverkehrsfluss). Weitere Informationen finden Sie unter Geoproximity-Routing sowie unter Dokumentformat für Datenverkehrsrichtlinien.

22. März 2023

Der gesamte Route-53-Leitfaden wurde mit der neuen Konsolenumgebung für Domains aktualisiert. Sie können die neue Konsolenoberfläche auch verwenden, um eine Domain von einer AWS-Konto zur anderen zu übertragen. AWS-Konto Weitere Informationen erhalten Sie unter Registrieren einer neuen Domain und Übertragen von Domänen.

10. März 2023

Sie können jetzt mithilfe IPv4 von,, oder Dual-Stack-Endpunkten mit Route 53 VPC Resolver eine Verbindung zu Ihren Ressourcen herstellen. IPv6 Weitere Informationen erhalten Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben und Werte, die Sie beim Erstellen oder Bearbeiten von ausgehenden Endpunkten angeben.

2022 Veröffentlichungen

21. September 2022

Sie können jetzt Richtlinienbedingungen verwenden, um Benutzern einen differenzierten Zugriff auf die Aktualisierung von Ressourcendatensätzen in Amazon Route 53 zu gewähren. Weitere Informationen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle.

30. August 2022

Amazon Route 53 unterstützt jetzt Aliaseinträge für AWS App Runner Services, die nach dem 1. August 2022 erstellt wurden. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an einen AWS App Runner Dienst.

1. Juni 2022

Die IP-basierte Routing-Option ist jetzt in Amazon Route 53 verfügbar. Weitere Informationen finden Sie unter IP-basiertes Routing.

16. März 2022

Geolokalisierungs- und latenzbasierte Routing-Optionen werden jetzt für private gehostete Zonen in Amazon Route 53 unterstützt. Weitere Informationen finden Sie unter Überlegungen zum Arbeiten mit einer privaten gehosteten Zone.

25 Januar 2022

Der Prozess für den Eigentümerwechsel für .com.au und .net.au TLDs wurde vereinfacht und umfasst nun auch die Beantwortung von zwei E-Mails (sowohl von alten als auch von neuen Registranten). Das Ausfüllen von Formularen ist nicht vorgesehen. Weitere Informationen erhalten Sie unter .com.au (Australien) und .net.au (Australien).

2021 Releases

26. Oktober 2021

Das Deaktivieren der standardmäßigen Reverse-DNS-Regeln mit Amazon Route 53 wird jetzt unterstützt. Sie können jetzt die Erstellung dieser Regeln deaktivieren und stattdessen Abfragen nach Reverse-DNS-Namespaces an externe Server weiterleiten, falls gewünscht. Weitere Informationen finden Sie unter Weiterleitungsregeln für Reverse-DNS-Abfragen in VPC Resolver.

1. September 2021

Es wurde ein neues Einstiegsthema hinzugefügt, das Sie durch die Erstellung von CloudFront Amazon-Distributionen für eine statische Website führt. Weitere Informationen finden Sie unter Verwenden Sie eine CloudFront Amazon-Distribution, um eine statische Website bereitzustellen.

14. Juli 2021

Die Nachverfolgung AWS verwalteter Richtlinien für Amazon Route 53 wurde gestartet. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon Route 53.

31. März 2021

Die Resolver-DNS-Firewall wurde hinzugefügt. Mit der DNS-Firewall können Sie Schutz für ausgehende DNS-Anfragen von Ihrem bieten. VPCs Weitere Informationen finden Sie unter Verwenden der DNS-Firewall zum Filtern von ausgehendem DNS-Verkehr.

Versionspunkte 2020

17. Dezember 2020

Unterstützung für DNSSEC-Signatur für Route 53 VPC Resolver hinzugefügt. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

Unterstützung für DNSSEC-Validierung für Route 53 VPC Resolver hinzugefügt. Weitere Informationen finden Sie unter Aktivieren der DNSSEC-Validierung in Amazon Route 53.

23. September 2020

Aktualisierung des gesamten Route 53 — Leitfadens mit der neuen Konsolenumgebung. Weitere Informationen finden Sie unter Was ist Amazon Route 53?.

1. September 2020

Unterstützung für Resolver-Abfrageprotokolle hinzugefügt. Weitere Informationen finden Sie unter Abfrageprotokollierung.

Versionen 2018

20. Dezember 2018

Sie können Route 53-Aliaseinträge erstellen, die den Datenverkehr an API Gateway APIs oder an Amazon VPC-Schnittstellenendpunkte weiterleiten. Weitere Informationen finden Sie unter Bewerten/Weiterleiten des Datenverkehrs an.

28. November 2018

Route 53 Auto Naming (auch bekannt als Service Discovery) ist jetzt ein separater Service. AWS Cloud Map Weitere Informationen finden Sie im AWS Cloud Map -Entwicklerhandbuch.

19. November 2018

Mit dem Route 53 Resolver können Sie die DNS-Auflösung zwischen Ihrer VPC und Ihrem Netzwerk über Direct Connect oder eine VPN-Verbindung konfigurieren. (Resolver ist der neue Name für den rekursiven DNS-Service, der standardmäßig allen Kunden in Amazon Virtual Private Cloud (Amazon VPC) zur Verfügung gestellt wird.) Auf diese Weise können Sie DNS-Anfragen von Resolvern in Ihrem Netzwerk an Route 53-Resolver weiterleiten. Mit dem Resolver können Sie auch Abfragen nach ausgewählten Domänennamen (example.com)

und Subdomänennamen (api.example.com) von einer VPC an Resolver in Ihrem Netzwerk weiterleiten. Weitere Informationen finden Sie unter Was ist Route 53 VPC Resolver?.

7. November 2018

Wenn Sie den Datenverkehrsfluss von Route 53 und die Weiterleitung aufgrund der geografischen Nähe verwenden, können Sie eine interaktive Karte verwenden, um die Weiterleitung Ihrer Endbenutzer zu Ihren Endpunkten auf der ganzen Welt zu visualisieren. Weitere Informationen finden Sie unter Anzeigen einer Karte, die die Auswirkungen der Einstellungen für geografische Nähe darstellt.

18. Oktober 2018

Sie können die Route 53-Konsole und die API verwenden, um eine Route 53-Zustandsprüfung vorübergehend zu deaktivieren. Auf diese Weise können Sie die Überwachung eines Endpunkts (z. B. ein Webserver) einfach unterbrechen, um eine Wartung durchzuführen, ohne Alarme auszulösen oder unnötige Protokolle oder Statusmeldungen zu erzeugen. Weitere Informationen finden Sie im Abschnitt „Deaktiviert“ unter Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen. Die Funktion ist für alle drei Arten von Route 53-Zustandsprüfungen verfügbar: Integritätsprüfungen, die einen Endpunkt überwachen, Integritätsprüfungen, die andere Zustandsprüfungen überwachen, und Integritätsprüfungen, die einen CloudWatch Alarm überwachen.

13. März 2018

Wenn Sie die automatische Benennung verwenden, können Sie jetzt den stabilheitscheck eines Drittanbieters verwenden, um den Zustand Ihrer Ressourcen zu bewerten. Dies ist nützlich, wenn eine Ressource nicht über das Internet verfügbar ist, z. B. weil sich die Instance in einer Amazon VPC befindet. Weitere Informationen finden Sie HealthCheckCustomConfigin der Amazon Route 53 API-Referenz.

9. März 2018

IAM enthält jetzt verwaltete Richtlinien für die automatische Benennung. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon Route 53.

6. Februar 2018

Sie können nun die automatische Benennung konfigurieren, um Aliasdatensätze zu erstellen, die den Datenverkehr an ELB-Load Balancer weiterleiten oder CNAME-Datensätze erstellen. Weitere Informationen finden Sie unter Attribute in der Dokumentation zur RegisterInstanceAPI in der Amazon Route 53 API-Referenz.

Versionen 2017

5. Dezember 2017

Sie können jetzt die Route 53-Autonaming-API für die Bereitstellung von Instances für Microservices verwenden. Mit Autonaming können Sie automatisch DNS-Datensätze erstellen und optional Zustandsprüfungen auf der Grundlage einer von Ihnen definierten Vorlage durchführen. Weitere Informationen finden Sie unter Was ist AWS Cloud Map? im AWS Cloud Map Entwicklerhandbuch.

16. November 2017

Sie können jetzt programmgesteuert die aktuellen Kontingente von Route 53-Ressourcen abrufen, wie etwa gehostete Zonen und Zustandsprüfungen sowie die Anzahl der einzelnen Ressourcen, die Sie derzeit nutzen. Weitere Informationen finden Sie unter GetAccountLimitGetHostedZoneLimit, und GetReusableDelegationSetLimitin der Amazon Route 53 API-Referenz.

3. Oktober 2017

Route 53 ist jetzt ein HIPAA-berechtigter Service. Weitere Informationen finden Sie unter Compliance-Validierung für Amazon Route 53.

29. September 2017

Sie können jetzt programmgesteuert überprüfen, ob eine Domäne zu Route 53 übertragen werden kann. Weitere Informationen finden Sie CheckDomainTransferabilityin der Amazon Route 53 API-Referenz.

11. September 2017

Sie können jetzt Route 53-Alias-Datensätze erstellen, die Internetdatenverkehr an Elastic Load Balancing Netzwerklastenausgleichsprogramme weiterleiten. Weitere Informationen zu Alias-Datensätzen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

7. September 2017

Wenn Sie Route 53 als öffentlichen, autoritativen DNS-Service verwenden, können Sie jetzt DNS-Anfragen eingeben, die Route 53 erhält. Weitere Informationen finden Sie unter Öffentliche DNS-Abfrageprotokollierung.

1. September 2017

   Wenn Sie den Route 53-Datenfluss verwenden, können Sie jetzt Geoproximity Routing verwenden, das Ihnen erlaubt, Datenverkehr auf der Grundlage der physischen Entfernung zwischen Ihren Nutzern und Ihren Ressourcen weiterzuleiten. Sie können auch mehr oder weniger Datenverkehr zu jeder Ressource leiten, indem Sie einen positiven oder negativen Bias-Wert angeben. Weitere Informationen finden Sie unter Geoproximity-Routing.

21. August 2017

   Sie können jetzt mit Route 53 Certification Authority Authorization (CAA)-Datensätze erstellen, die Ihnen ermöglichen, die Zertifikatsautoritäten anzugeben, die Zertifikate für Ihre Domänen und Subdomänen ausgeben können. Weitere Informationen finden Sie unter CAA-Datensatztyp.

18. August 2017

   Sie können jetzt große Zahlen von Domänen mit der Route 53-Konsole zu Route 53 übertragen. Weitere Informationen finden Sie unter Übertragen der Registrierung für eine Domain an Amazon Route 53.

4. August 2017

   Wenn Sie eine Domain registrieren, müssen Sie bei den Registrierungen einiger Top-Level-Domains (TLDs) verifizieren, dass Sie eine gültige E-Mail-Adresse für den Ansprechpartner des Registranten angegeben haben. Sie können jetzt die Bestätigungs-E-Mail-Nachricht senden und erhalten eine Bestätigung, dass Sie die E-Mail-Adresse während der Domänenregistrierung erfolgreich geprüft haben. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

21. Juni 2017

   Wenn Sie Datenverkehr praktisch zufällig zu mehreren Ressourcen weiterleiten möchten, beispielsweise zu Webservern, können Sie jetzt einen mehrwertigen Antwortdatensatz für jede Ressource erstellen und optional jedem Datensatz eine Route 53-Zustandsprüfung zuordnen. Route 53 beantwortet DNS-Abfragen mit bis zu acht fehlerfreien Datensätzen und gibt verschiedenen DNS-Resolvern verschiedene Antworten. Weitere Informationen finden Sie unter Mehrwertiges Antwort-Routing.

10. April 2017

   Wenn Sie die Route 53-Konsole verwenden, um eine Domänenregistrierung in Route 53 zu übertragen, können Sie jetzt eine der folgenden Optionen zum Verknüpfen der Namensserver für den DNS-Service für die Domäne mit der übertragenen Domänenregistrierung verwenden:

- Verwenden Sie die Namenserver für eine von Ihnen ausgewählte gehostete Route 53-Zone:
- Verwenden Sie die Namensserver für den aktuellen DNS-Service für die Domäne
- Verwenden Sie Namensserver, die Sie angeben

Route 53 ordnet diese Namensserver automatisch mit der übertragenen Domänenregistrierung zu.

Versionen 2016

21. November 2016

Sie können jetzt Integritätsprüfungen erstellen, bei denen IPv6 Adressen verwendet werden, um den Zustand von Endgeräten zu überprüfen. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

15. November 2016

Sie können nun mithilfe einer Route 53-API-Aktion eine Amazon VPC, die Sie mit einem Konto erstellt haben, mit einer privat gehosteten Zone verknüpfen, die Sie mit einem anderen Konto erstellt haben. Weitere Informationen finden Sie unter Zuordnen einer Amazon VPC und einer privaten gehosteten Zone, die Sie mit verschiedenen Konten erstellt haben AWS.

30. August 2016

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Name Authority Pointer (NAPTR)-Datensätze - Sie können jetzt NAPTR-Datensätze erstellen, die von Dynamic Delegation Discovery System (DDDS)-Anwendungen genutzt werden, um einen Wert in einen anderen zu konvertieren oder einen Wert durch einen anderen zu ersetzen. Eine gängige Anwendung ist beispielsweise die Konvertierung von Telefonnummern in SIP URIs. Weitere Informationen finden Sie unter NAPTR-Datensatztyp.
- DNS-Abfrage-Testtool - Sie können jetzt DNS-Abfragen für einen Datensatz simulieren und sehen, welchen Wert Route 53 zurückgibt. Für Geolokalisierungs- und Latenzdaten können Sie auch Anfragen von einer bestimmten and/or DNS-Resolver-Client-IP-Adresse simulieren, um herauszufinden, welche Antwort Route 53 an einen Client mit dieser and/or Resolver-IP-Adresse zurückgeben würde. Weitere Informationen finden Sie unter Überprüfen der DNS-Antworten von Route 53.

11. August 2016

Ab dieser Version können Sie Alias-Datensätze erstellen, die den Datenverkehr an ELB Application Load Balancer weiterleiten. Der Vorgang ist mit dem für Classic Load Balancer identisch. Weitere Informationen finden Sie unter Bewerten/Weiterleiten des Datenverkehrs an.

9. August 2016

Ab dieser Version fügt Route 53 Unterstützung für DNSSEC für die Domänenregistrierung hinzu. Mit DNSSEC können Sie Ihre Domain vor DNS-Spoofing-Angriffen schützen, die auch als Angriffe bezeichnet werden. man-in-the-middle Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

7. Juli 2016

Sie können jetzt die Registrierung für eine Domäne manuell erweitern und eine Domäne mit einer ersten Registrierungsdauer länger als die minimale von der Registrierung angegebene Registrierungsdauer registrieren. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

6. Juli 2016

Wenn Sie ein AISPL-Kunde mit einer Kontaktadresse in Indien sind, können Sie nun mithilfe von Route 53 Domänen registrieren. Weitere Informationen finden Sie unter Verwalten eines Kontos in Indien.

26. Mai 2016

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Domänen-Rechnungsbericht - Sie können jetzt einen Bericht herunterladen, der alle Domänenregistrierungsgebühren nach Domäne für einen bestimmten Zeitraum auflistet. Der Bericht umfasst alle gebührenpflichtigen Domainregistrierungsvorgänge, einschließlich der Registrierung von Domains, der Übertragung von Domains auf Route 53, der Verlängerung der Domainregistrierung und (für einige TLDs) der Wechsel des Inhabers einer Domain. Weitere Informationen finden Sie in der folgenden Dokumentation:
  - Route 53— SieheHerunterladen von Domains-Rechnungsberichten
  - Route 53-API — Weitere Informationen finden Sie ViewBillingin der Amazon Route 53-API-Referenz.
- Neu TLDs — Sie können jetzt Domains registrieren, die Folgendes haben TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website

und .uk. Weitere Informationen finden Sie unter Domains, die Sie mit Amazon Route 53 registrieren können.

- Neu APIs bei der Domainregistrierung — Bei Vorgängen, bei denen bestätigt werden muss, dass die E-Mail-Adresse für den Registrantenkontakt gültig ist, z. B. bei der Registrierung einer neuen Domain, können Sie jetzt programmgesteuert feststellen, ob der Kontakt des Registranten auf den Link in der Bestätigungs-E-Mail geklickt hat und, falls nicht, ob der Link noch gültig ist. Sie können auch programmgesteuert anfordern, dass wir eine weitere Bestätigungs-E-Mail senden. Weitere Informationen finden Sie in der folgenden Dokumentation im.Amazon Route 53 — API-Referenz:
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

5. April 2016

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Zustandsprüfungen auf der Grundlage von CloudWatch Metriken — Sie können jetzt Zustandsprüfungen erstellen, die auf dem Alarmstatus einer beliebigen CloudWatch Metrik basieren. Damit können Sie den Zustand der Endpunkte überprüfen, die nicht durch eine herkömmliche Route 53-Zustandsprüfung erreicht werden, wie Instances in einer Amazon Virtual Private Cloud (VPC), die nur über private IP-Adressen verfügen. Weitere Informationen finden Sie in der folgenden Dokumentation:
  - Route 53-Konsole - Siehe Überwachung von CloudWatch-Alarmen im Thema "Angegebene Werte beim Erstellen oder Aktualisieren von Zustandsprüfungen".
  - Route 53-API — Weitere Informationen finden Sie unter CreateHealthCheckund UpdateHealthCheckin der Amazon Route 53-API-Referenz.
- Konfigurierbare Standorte für die Zustandsprüfung - Sie haben die Möglichkeit, die Route 53-Zustandsprüfungsregionen festzulegen, die den Status Ihrer Ressourcen überprüfen, was die Verarbeitungslast von Zustandsprüfungen am Endpunkt verringert. Dies ist nützlich, wenn Ihre Kunden in einer oder mehreren geografischen Regionen konzentriert sind. Weitere Informationen finden Sie in der folgenden Dokumentation:
  - Route 53-Konsole - Siehe Erweiterte Konfiguration (nur "Monitor an endpoint") im Thema "Angegebene Werte beim Erstellen oder Aktualisieren von Zustandsprüfungen".
  - Route 53-API — Weitere Informationen finden Sie im `Regions` Element für CreateHealthCheckund UpdateHealthCheckin der Amazon Route 53-API-Referenz.
- Failover in privat gehosteten Zonen - Sie können jetzt Failover- und Failover-Alias-Datensätze in einer privat gehosteten Zone erstellen. Wenn Sie dieses Feature mit der Metrik-

basierten Zustandsprüfungen kombinieren, können Sie DNS-Failover selbst für Endpunkte konfigurieren, die nur über private IP-Adressen verfügen und mithilfe von Standard-Route 53-Zustandsprüfungen nicht erreicht werden können. Weitere Informationen finden Sie in der folgenden Dokumentation:

- Route 53— SieheKonfigurieren von Failover in einer privaten gehosteten Zoneaus.
- Route 53-API — Weitere Informationen finden Sie ChangeResourceRecordSetsin der Amazon Route 53-API-Referenz.

- Alias-Datensätze in privat gehosteten Zonen - Bisher konnten Sie Alias-Datensätze erstellen, die DNS-Abfragen nur an andere Route 53 -Datensätze in derselben Hosting-Zone weiterleiten. Ab dieser Version können Sie auch Alias-Datensätze erstellen, die DNS-Abfragen an Elastic Beanstalk-Umgebungen weiterleiten, die regionalisierte Subdomänen, Elastic Load Balancer und Amazon-S3-Buckets enthalten. (Sie können immer noch keine Alias-Einträge erstellen, die DNS-Abfragen an eine CloudFront Distribution weiterleiten.) Weitere Informationen finden Sie in der folgenden Dokumentation:
  - Route 53— SieheWählen zwischen Alias- und Nicht-Alias-Datensätzenaus.
  - Route 53-API — Weitere Informationen finden Sie ChangeResourceRecordSetsin der Amazon Route 53-API-Referenz.

23. Februar 2016

Wenn Sie HTTPS-Zustandsprüfungen erstellen oder aktualisieren, können Sie Route 53 nun so konfigurieren, dass der Host-Name während der TLS-Aushandlung an den Endpunkt gesendet wird. Dadurch kann der Endpunkt auf die HTTPS-Anfrage mit dem entsprechenden SSL/TLS Zertifikat antworten. Weitere Informationen finden Sie in der Beschreibung für das Erweiterte Konfiguration (nur "Monitor an endpoint") Feld SNI im Thema „Werte, die Sie beim Erstellen oder Aktualisieren von Integritätsprüfungen angeben“. Informationen darüber, wie Sie SNI aktivieren, wenn Sie die API verwenden, um eine Zustandsprüfung zu erstellen oder zu aktualisieren, finden Sie unter CreateHealthCheckund UpdateHealthCheckin der Amazon Route 53 API-Referenz.

27. Januar 2016

Sie können jetzt Domains für über 100 zusätzliche Top-Level-Domains (TLDs) wie .accountants, .band und .city registrieren. Eine vollständige Liste der unterstützten Programme finden Sie unter. TLDs Domains, die Sie mit Amazon Route 53 registrieren können

19. Januar 2016

Sie können jetzt Alias-Datensätze erstellen, die Datenverkehr an Elastic Beanstalk-Umgebungen weiterleiten. Informationen zur Erstellung von Datensätzen mit der Route 53-Konsole finden

Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole. Informationen zur Verwendung der API zum Erstellen von Datensätzen finden Sie ChangeResourceRecordSetsin der Amazon Route 53 API-Referenz.

Versionen 2015

3. Dezember 2015

Die Route 53-Konsole enthält jetzt einen visuellen Editor, mit dem Sie schnell komplexe Routing-Konfigurationen erstellen können, die eine Kombination von gewichteten, Latenz-, Failover- und Geolocation-Routing-Richtlinien aus Route 53 verwenden. Sie können dann die Konfiguration mit einem oder mehreren Domänennamen (z. B. beispiel.com) oder Subdomänen-Namen (z. B. www.beispiel.com) in derselben gehosteten Zone oder in mehreren gehosteten Zonen verknüpfen. Außerdem können Sie ein Rollback der Aktualisierungen durchführen, wenn die neue Konfiguration sich nicht wie erwartet verhält. Dieselbe Funktionalität ist verfügbar, wenn Sie die Route 53-API AWS SDKs, AWS CLI, und verwenden AWS Tools for Windows PowerShell. Weitere Informationen zur Verwendung des visuellen Editors finden Sie unter Verwenden von Traffic Flow zum Weiterleiten von DNS-Verkehr. Weitere Informationen zur Verwendung der API für Datenverkehrsfluss-Konfigurationen finden Sie im.Amazon Route 53 — API-Referenzaus.

19. Oktober 2015

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Domainregistrierung für.com- und .net-Domains durch Amazon Registrar, Inc. — Amazon ist jetzt ein von der ICANN akkreditierter Registrar für die Top-Level-Domains .com und .net (TLDs) über Amazon Registrar, Inc. Wenn Sie Route 53 zur Registrierung einer.com- oder .net-Domain verwenden, ist Amazon Registrar der registrierte Registrar und wird in Ihren Whois-Abfrageergebnissen als „Sponsoring Registrar“ aufgeführt. Weitere Informationen zur Verwendung von Route 53 zur Domänenregistrierung finden Sie unter Registrieren und Verwalten von Domainnamen unter Verwendung von Amazon Route 53.
- Datenschutz für .com- und .net-Domänen - Wenn Sie eine .com- und .net-Domäne bei Route 53 registrieren, werden alle Ihre persönlichen Informationen, einschließlich Vor- und Nachname, jetzt ausgeblendet. Vor- und Nachname werden nicht für andere Domänen verborgen, die Sie bei Route 53 registrieren. Weitere Informationen zum Datenschutz finden Sie unter Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne.

15. September 2015

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Berechnete Zustandsprüfungen - Sie können jetzt Zustandsprüfungen erstellen, deren Status durch den Zustand anderer Zustandsprüfungen bestimmt wird. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen. Weitere Informationen finden Sie CreateHealthCheckin der Amazon Route 53 API-Referenz.
- Latenzmessungen für Zustandsprüfungen - Sie können jetzt Route 53 konfigurieren, um die Latenz zwischen Zustandsprüfung und Ihrem Endpunkt zu messen. Latenzdaten werden in Amazon CloudWatch Graphs in der Route 53-Konsole angezeigt. Informationen zum Aktivieren der Latenzmessungen für neue Zustandsprüfungen finden Sie unter der Einstellung für Latenzmessungen unter Erweiterte Konfiguration (nur "Monitor an endpoint") im Thema Werte, die Sie beim Erstellen oder Aktualisieren von Zustandsprüfungen festlegen. (Sie können Latenzmessungen nicht für vorhandene Zustandsprüfungen aktivieren.) Weitere Informationen finden Sie MeasureLatencyim Thema CreateHealthCheckin der Amazon Route 53 API-Referenz.
- Aktualisierungen des Dashboards für Zustandsprüfungen in der Route 53-Konsole — Das Dashboard für die Überwachung von Zustandsprüfungen wurde in vielerlei Hinsicht verbessert, einschließlich CloudWatch Grafiken zur Überwachung der Latenz zwischen Route 53-Zustandsprüfern und Ihren Endpunkten. Weitere Informationen finden Sie unter Den Status von Zustandsprüfungen überwachen und Benachrichtigungen erhalten.

3. März 2015

Das Amazon Route 53 Entwicklerhandbuch enthält jetzt Erläuterungen zur Konfiguration von White Label-Nameservern für gehostete Route 53-Zonen. Weitere Informationen finden Sie unter Konfigurieren von White-Label-Nameservern.

26. Februar 2015

Sie können jetzt die Route 53-API verwenden, um die gehosteten Zonen, die einem AWS Konto zugeordnet sind, in alphabetischer Reihenfolge nach Namen aufzulisten. Sie können auch die Anzahl der gehosteten Zonen abrufen, die mit einem Konto verknüpft sind. Weitere Informationen finden Sie unter ListHostedZonesByNameund GetHostedZoneCountin der Amazon Route 53 API-Referenz.

11. Februar 2015

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Zustandsprüfungs-Status - Die Seite für Zustandsprüfungen in der Route 53-Konsole enthält jetzt eine Status-Spalte, mit der Sie den Gesamtstatus Ihrer Zustandsprüfungen anzeigen können. Weitere Informationen finden Sie unter Anzeigen von Zustandsprüfungsstatus und dem Grund für Zustandsprüfungsausfälle.

- Integration mit AWS CloudTrail — Route 53 funktioniert jetzt mit CloudTrail , um Informationen zu jeder Anfrage zu erfassen, die Ihr AWS Konto an die Route 53-API sendet. Durch die Integration von Route 53 CloudTrail können Sie feststellen, welche Anfragen an die Route 53-API gestellt wurden, von welcher Quell-IP-Adresse jede Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und vieles mehr. Weitere Informationen finden Sie unter Protokollieren von Amazon Route 53-API-Aufrufen mit AWS CloudTrail.
- Schnellalarme für Zustandsprüfungen — Wenn Sie mithilfe der Route 53-Konsole eine Zustandsprüfung erstellen, können Sie jetzt gleichzeitig einen CloudWatch Amazon-Alarm für die Zustandsprüfung erstellen und angeben, wer benachrichtigt werden soll, wenn Route 53 den Endpunkt für eine Minute als fehlerhaft einstuft. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.
- Tagging für gehostete Zonen und Domänen - Sie können jetzt Tags, die häufig für die Kostenzuordnung verwendet werden, an gehostete Route 53-Zonen und Domänen zuweisen. Weitere Informationen finden Sie unter Amazon-Route-53-Ressourcen-Markierung.

5. Februar 2015

Sie können jetzt mit der Route 53-Konsole die Kontaktinformationen für eine Domäne aktualisieren. Weitere Informationen finden Sie unter Angegebene Werte beim Registrieren oder Übertragen einer Domain.

22. Januar 2015

Sie können jetzt internationalisierte Domänennamen angeben, wenn Sie einen neuen Domänennamen bei Route 53 registrieren. (Route 53 hat bereits internationalisierte Domänennamen für gehostete Zonen und Datensätze unterstützt.) Weitere Informationen finden Sie unter Format für DNS-Domänennamen.

Versionen 2014

25. November 2014

Mit dieser Version können Sie hetzt den Kommentar bearbeiten, den Sie für eine gehostete Zone beim Erstellen angegeben haben. Klicken Sie in der Konsole einfach auf das Stiftsymbol neben dem Kommentarfeld, und geben Sie einen neuen Wert ein. Weitere Informationen zum Ändern des Kommentars mithilfe der Route 53-API finden Sie UpdateHostedZoneCommentin der Amazon Route 53-API-Referenz.

5. November 2014

Mit dieser Version verfügt Route 53 über die folgenden neuen Funktionen:

- Privates DNS, das mit dem Amazon Virtual Private Cloud Cloud-Dienst VPCs erstellt wurde — Sie können jetzt Route 53 verwenden, um Ihre internen Domainnamen zu verwalten, VPCs ohne DNS-Daten dem öffentlichen Internet zugänglich zu machen. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.
- Zustandsprüfungs-Fehlerursachen - Sie können jetzt den aktuellen Status einer ausgewählten Zustandsprüfung und Details zu den letzten Fehlerursachen in der Zustandsprüfung anzeigen, die von jeder Route 53-Zustandsprüfung gemeldet werden. Der Status enthält den HTTP-Statuscode, und Fehlerursachen enthalten Informationen über verschiedene Arten von Fehlern, wie zum Beispiel mit Zeichenfolgenabgleich-Fehler und Zeitüberschreitungen. Weitere Informationen finden Sie unter Anzeigen von Zustandsprüfungsstatus und dem Grund für Zustandsprüfungsausfälle.
- Wiederverwendbare Delegationssätze - Sie können nun dieselbe Gruppe von vier autoritativen Namensservern, zusammenfassend als Delegationssatz bezeichnet, auf mehrere gehostete Zonen anwenden, die unterschiedlichen Domänennamen entsprechen. Dies vereinfacht den Prozess der Migration des DNS-Service zu Route 53 und die Verwaltung einer großen Anzahl von gehosteten Zonen. Die Verwendung von wiederverwendbaren Delegierungssätzen erfordert derzeit, dass Sie die Route 53-API oder ein AWS -SDK verwenden. Weitere Informationen finden Sie unter Amazon Route 53 API Reference.
- Verbessertes Geolocation-Routing — Wir haben die Genauigkeit des Geolocation-Routing weiter verbessert, indem wir Unterstützung für die Erweiterung von EDNS0 hinzugefügt haben. edns-client-subnet Weitere Informationen finden Sie unter Geolocation-Routing.
- Unterstützung für Signature v4 - Sie können jetzt alle Route 53-API-Anforderungen mithilfe von Signature Version 4 signieren. Weitere Informationen finden Sie unterSignieren von Route 53 API-AnforderungenimAmazon Route 53 — API-Referenzas.

31. Juli 2014

Ab dieser Version können Sie jetzt Folgendes ausführen:

- Registrieren neuer Domänennamen mithilfe von Amazon Route 53. Weitere Informationen finden Sie unter Registrieren und Verwalten von Domainnamen unter Verwendung von Amazon Route 53.
- Konfigurieren von Route 53, um DNS-Abfragen basierend auf dem geografischen Standort zu beantworten, von dem die Abfragen stammen. Weitere Informationen finden Sie unter Geolocation-Routing.

2. Juli 2014

Ab dieser Version können Sie jetzt Folgendes ausführen:

- Bearbeiten der meisten Werte in Zustandsprüfungen. Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.
- Verwenden der Route 53-API, um eine Liste der IP-Bereiche abzurufen, die Route 53-Zustandsprüfungen verwenden, um den Status Ihrer Ressourcen zu überprüfen. Sie können diese IP-Adressen zur Konfiguration Ihrer Router- und Firewall-Regeln verwenden, um es der Zustandsprüfung zu ermöglichen, den Zustand Ihrer Ressourcen zu überprüfen. Weitere Informationen finden Sie GetCheckerIpRangesin der Amazon Route 53 API-Referenz.
- Weisen Sie den Zustandsprüfungen Kostenzuordnungs-Tags zu, mit denen Sie den Zustandsprüfungen auch einen Namen zuweisen können. Weitere Informationen finden Sie unter Benennen und Verwenden von Tags für Zustandsprüfungen.
- Verwenden Sie die Route 53-API, um die Anzahl der Gesundheitschecks abzurufen, die mit Ihrem AWS Konto verknüpft sind. Weitere Informationen finden Sie GetHealthCheckCountin der Amazon Route 53 API-Referenz.

30. April 2014

Mit dieser Version können Sie jetzt Zustandsprüfungen erstellen und einen Domänennamen anstelle einer IP-Adresse verwenden, um den Endpunkt anzugeben. Dies ist hilfreich, wenn die IP-Adresse eines Endpunkts entweder nicht festgelegt ist oder von mehreren IPs, z. B. Amazon EC2 - oder Amazon RDS-Instances, bedient wird. Weitere Informationen finden Sie unter Erstellen und Aktualisieren von Zustandsprüfungen.

Außerdem wurden einige Informationen zur Verwendung der Route 53-API, die früher im Amazon Route 53-Benutzerhandbuch angegeben waren, verschoben. Jetzt erscheint die gesamte API-Dokumentation im.Amazon Route 53 — API-Referenzaus.

18. April 2014

Ab dieser Version übergibt Route 53 einen anderen Wert in der `Host`-Kopfzeile, wenn in der Zustandsprüfung der Wert für Port 443 ist und der Wert für Protokoll HTTPS. Während einer Zustandsprüfung übergibt Route 53 nun eine `Host`-Kopfzeile an den Endpunkt, die den Wert des Felds Host Name enthält. Wenn Sie die Zustandsprüfung mithilfe der `CreateHealthCheck` API-Aktion erstellt haben, ist dies der Wert des Elements `FullyQualifiedDomainName`.

Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

9. April 2014

Mit dieser Version können Sie jetzt ansehen, welcher Prozentsatz der Route 53-Zustandsprüfungen derzeit meldet, dass ein Endpunkt betriebsbereit ist.

Darüber hinaus zeigt das Verhalten der Health Check-Status-Metrik in Amazon CloudWatch jetzt nur noch Null (wenn Ihr Endpunkt während eines bestimmten Zeitraums fehlerhaft war) oder Eins (wenn der Endpunkt in diesem Zeitraum fehlerfrei war). Die Metrik zeigt nicht mehr Werte zwischen 0 und 1 an, um den Anteil der Route 53-Zustandsprüfungen widerzuspiegeln, die den Endpunkt als fehlerfrei melden.

Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

18. Februar 2014

Mit dieser Version verfügt Route 53 über die folgenden Funktionen:

- Failover-Schwellenwert der Zustandsprüfung: Sie können jetzt angeben, wie viele aufeinander folgende Zustandsprüfungen ein Endpunkt nicht bestehen muss, bevor Route 53 den Endpunkt als fehlerhaft betrachtet – zwischen 1 und 10 aufeinander folgende Prüfungen. Ein fehlerhafter Endpunkt muss die gleiche Anzahl von Prüfungen bestehen, um als fehlerfrei zu gelten. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.
- Anforderungsintervall der Zustandsprüfung: Sie können jetzt angeben, wie häufig Route 53 Anforderungen an einen Endpunkt sendet, um festzustellen, ob der Endpunkt fehlerfrei ist. Gültige Einstellungen sind 10 Sekunden und 30 Sekunden. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

30. Januar 2014

Mit dieser Version verfügt Route 53 über die folgenden Funktionen:

- HTTP- und HTTPS-Zeichenfolgenübereinstimmungs-Zustandsprüfungen: Route 53 unterstützt jetzt Zustandsprüfungen, welche die Integrität eines Endpunkts basierend auf dem Erscheinungsbild einer bestimmten Zeichenfolge in der Antwort bestimmen. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.
- HTTPS-Zustandsprüfungen: Route 53 unterstützt jetzt Zustandsprüfungen für sichere SSL-Websites. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

- **`UPSERT`** für die **`ChangeResourceRecordSets`** API-Aktion: Beim Erstellen oder Ändern von Datensätzen über die `ChangeResourceRecordSets`-API-Aktion können Sie jetzt die Aktion `UPSERT` verwenden, um einen neuen Datensatz zu erstellen, falls noch keiner mit einem bestimmten Namen und Typ vorhanden ist, oder um einen vorhandenen Datensatz zu aktualisieren. Weitere Informationen finden Sie ChangeResourceRecordSetsin der Amazon Route 53 API-Referenz.

7. Januar 2014

Mit dieser Version von Route 53 wird Unterstützung für Zustandsprüfungen zur Integrität eines Endpunkts hinzugefügt, je nachdem, ob eine angegebene Zeichenfolge in der Antwort vorhanden ist. Weitere Informationen finden Sie unter So ermittelt Amazon Route 53, ob eine Zustandsprüfung fehlerfrei ist.

Versionen 2013

14. August 2013

Ab dieser Version fügt Route 53 Unterstützung für das Erstellen von Datensätzen durch Importieren einer Zonendatei im BIND-Format hinzu. Weitere Informationen finden Sie unter Erstellen von Datensätzen durch Importieren einer Zonendatei.

Darüber hinaus wurden CloudWatch Metriken für Route 53-Zustandsprüfungen in die Route 53-Konsole integriert und optimiert. Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

26. Juni 2013

Mit dieser Version bietet Route 53 Unterstützung für die Integration von Integritätsprüfungen in CloudWatch Metriken, sodass Sie Folgendes tun können:

- Überprüfen Sie, ob eine Zustandsprüfung korrekt konfiguriert ist.
- Überprüfen Sie den Status eines Zustandsprüfungs-Endpunkts über einen bestimmten Zeitraum.
- Konfigurieren CloudWatch Sie so, dass eine Amazon Simple Notification Service (Amazon SNS) -Warnung gesendet wird, wenn alle Route 53-Zustandsprüfungen Ihren angegebenen Endpunkt als fehlerhaft einstufen.

Weitere Informationen finden Sie unter Überwachung von Zustandsprüfungen mit CloudWatch.

11. Juni 2013

Mit dieser Version bietet Route 53 Unterstützung für die Erstellung von Aliaseinträgen, die DNS-Abfragen an alternative Domainnamen für CloudFront Amazon-Distributionen weiterleiten. Sie können dieses Feature sowohl für alternative Domainnamen im Zone Apex (example.com) und für alternative Domainnamen für Subdomains (www.example.com) verwenden. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

30. Mai 2013

Mit dieser Version bietet Route 53 Unterstützung für die Bewertung des Zustands von ELB-Load Balancern und den zugehörigen EC2 Amazon-Instances. Weitere Informationen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

28. März 2013

Die Dokumentation zu Zustandsprüfungen und Failover wurde für bessere Benutzerfreundlichkeit umgeschrieben. Weitere Informationen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

11. Februar 2013

Ab dieser Version fügt Route 53 Unterstützung für Failover und Zustandsprüfungen hinzu. Weitere Informationen finden Sie unter Amazon Route 53-Zustandsprüfungen erstellen .

Version 2012

21. März 2012

Ab dieser Version können Sie mit Route 53 Latenz-Datensätze erstellen. Weitere Informationen finden Sie unter Latenzbasiertes Routing.

Versionen 2011

21. Dezember 2011

In dieser Version AWS-Managementkonsole können Sie mit der Route 53-Konsole in einen Aliaseintrag erstellen, indem Sie einen Elastic Load Balancer aus einer Liste auswählen, anstatt die Hosting-Zonen-ID und den DNS-Namen des Load Balancers manuell einzugeben. Neue Funktionen werden im dokumentiert.Amazon Route 53 — Entwicklerhandbuchaus.

16. November 2011

Mit dieser Version können Sie die Route 53-Konsole in der verwenden, AWS-Managementkonsole um gehostete Zonen zu erstellen und zu löschen sowie Datensätze zu erstellen, zu ändern und zu löschen. Neue Funktionen wurden entsprechend im gesamten Amazon Route 53 Benutzerhandbuch dokumentiert.

18. Oktober 2011

DieAmazon Route 53 — Erste Schrittewurde in dieAmazon Route 53 — Entwicklerhandbuch, und dieEntwicklerhandbuchUm Folgendes anzuzeigen, wurde neu strukturiert.

24. Mai 2011

Diese Version von Amazon Route 53 führt Alias-Datensätze ein, mit deren Hilfe Sie Zone Apex-Aliasnamen, gewichtete Datensätze, eine neue API (2011-05-05) und Service Level Agreements erstellen können. Darüber hinaus ist Route 53 nach sechs Monaten in der Beta-Version nun allgemein verfügbar. Weitere Informationen finden Sie im .Amazon Route 53-ProduktseiteundWählen zwischen Alias- und Nicht-Alias-DatensätzenimAmazon Route 53 — Entwicklerhandbuchaus.

Version 2010

5. Dezember 2010

Dies ist die erste Veröffentlichung des Amazon Route 53-Entwicklerhandbuchs.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.