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 Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers beschrieben.

Weitere Funktionen von Route 53

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

Route 53 Resolver

Holen Sie sich rekursives DNS für Ihre Amazon-VPCs in AWS-Regionen, VPCs 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? Amazon Route 53 Resolver.

Amazon Route 53 Resolver auf Outposts-Endpunkten

Connect Route 53 Resolver auf Outpost-Racks über Route 53 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?.

Route 53 Resolver DNS Firewall

Schützen Sie Ihre rekursiven DNS-Abfragen innerhalb des Route 53 Resolvers. Erstellen Sie Domainlisten und erstellen Sie Firewallregeln, die ausgehenden DNS-Verkehr anhand dieser Regeln filtern.

Weitere Informationen finden Sie unter Route 53 Resolver DNS Firewall.

Datenverkehrsfluss

E asy-to-use - und kosteneffizientes globales Verkehrsmanagement: Leitet Endbenutzer auf der Grundlage von Geonähe, Latenz, Integrität und anderen Überlegungen zum besten Endpunkt für Ihre Anwendung weiter.

Weitere Informationen finden Sie unter Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr.

Amazon Route 53 53-Profile

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

Weitere Informationen finden Sie unter 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 Notebook bis hin zu Servern, die Inhalte für riesige Einzelhandels-Websites zur Verfügung stellen, kommunizieren über Zahlen miteinander. Diese Zahlen, bekannt als IP-Adressen, liegen in einem der folgenden Formate vor:

- Internetprotokoll Version 4 (IPv4), z. B. 192.0.2.44
- Internetprotokoll Version 6 (IPv6), z. B. 2001:0db8:85a3:0000:0000: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 zu leiten, der eine IPv4-IP-Adresse hat, geben Sie A als Typ ein.

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 als Typ angeben, geben Sie eine IP-Adresse im IPv4-Format ein, z. B. 192.0.2.136.

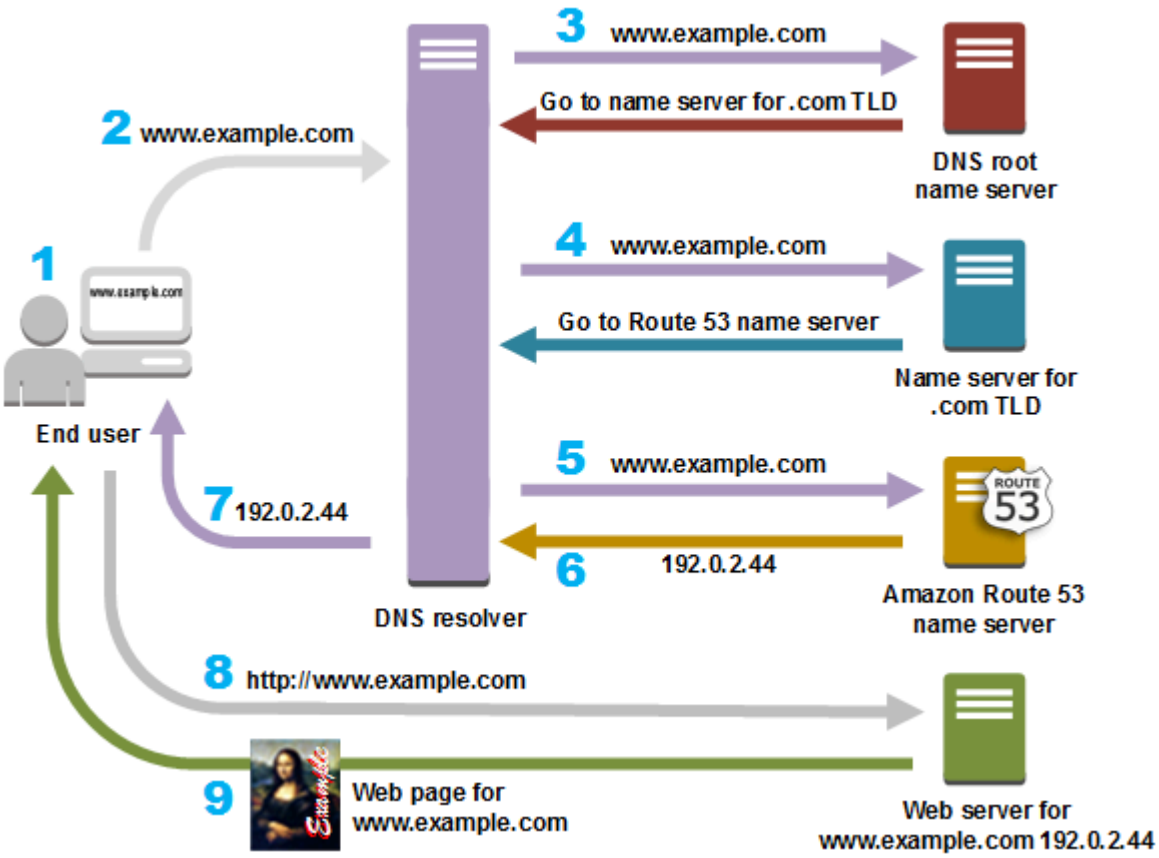
Weitere Informationen über Einträge finden Sie unter Arbeiten mit Datensätzen.

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 finden 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.

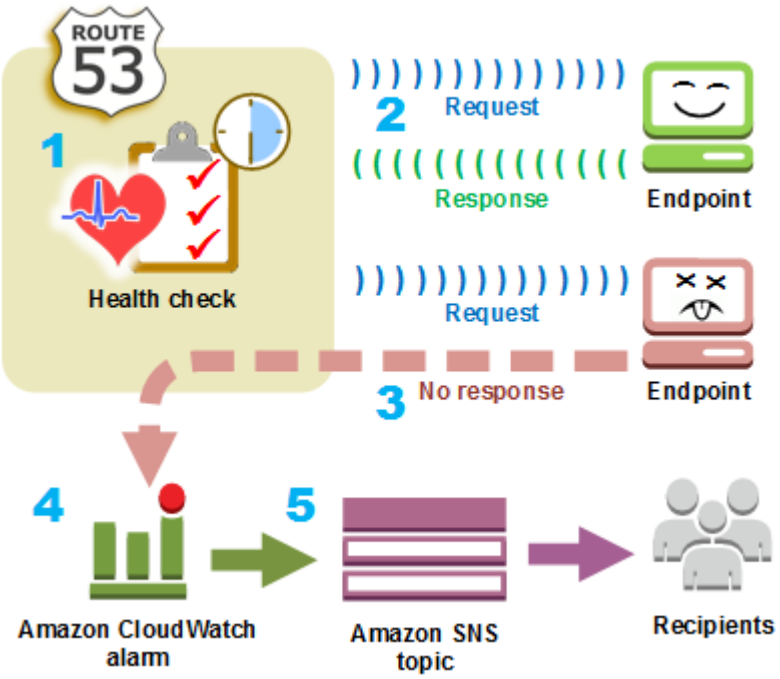
> **Note**
>
> Der DNS-Resolver behält außerdem die IP-Adresse für example.com für eine von Ihnen festgelegte Dauer im Zwischenspeicher, damit er schneller reagieren kann, wenn erneut ein Benutzer example.com aufruft. Weitere Informationen finden Sie unter time to live (TTL).

8. Der Webbrowser sendet eine Anforderung für www.example.com an die IP-Adresse, die er vom DNS-Resolver erhalten hat. Dort befindet sich Ihr Inhalt, beispielsweise ein Webserver, der auf einer Amazon-EC2-Instance ausgeführt wird, oder ein 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 Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

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 ICANN (Internet Corporation for Assigned Names and Numbers) für die Verarbeitung von Domänenregistrierungen für bestimmte Domänen der obersten Ebene (Top-Level-Domains, TLDs) zugelassen wurde. 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. Das 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 TLDs vermitteln in der Regel den Benutzern ein Bild 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 stehen im Zusammenhang mit geografischen Regionen wie Ländern oder Städten. Einige Registrierungen für geografische TLDs haben Residenzanforderungen, während andere, z. B. the section called “.io (Britisches Territorium im Indischen Ozean)”, als generische TLD zulässig oder sogar erwünscht sind.

Eine Liste der TLDs, die Sie verwenden können, wenn Sie einen Domänennamen mit Route 53 registrieren, 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 einen CIDR-Block von /0 bis /24 für IPv4 und /0 bis /48 für IPv6 angeben. Zum Beispiel enthält ein /24 IPv4 CIDR-Block 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:

- Internetprotokoll Version 4 (IPv4), z. B. 192.0.2.44
- Internetprotokoll Version 6 (IPv6), z. B. 2001:0db8:85a3:0000:0000:abcd:0001:2345

Route 53 unterstützt IPv4- und IPv6-Adressen für die folgenden Zwecke:

- Sie können Datensätze erstellen, die den Typ A für IPv4-Adressen oder den Typ AAAA für IPv6-Adressen haben.

- Sie können Zustandsprüfungen erstellen, die Anforderungen an IPv4- oder IPv6-Adressen senden.
- Wenn ein DNS-Auflöser sich in einem IPv6-Netzwerk befindet, kann er entweder IPv4 oder IPv6 zum Senden von Anfragen an Route 53 verwenden.

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 System (DNS), mit dem Sie den Datenverkehr für eine Domäne und deren Subdomänen an eine oder mehrere Amazon-EC2-Instances innerhalb von 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 CreateHostedZone und CreateReusableDelegationSetin der Amazon Route 53 API-Referenz. Das gleiche Feature finden Sie auch in den AWS -SDKs, in AWS Command Line Interface und 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:

- Für öffentliche und private DNS von Route 53 ist die Steuerebene die Route-53-Konsole und APIs, mit denen Sie DNS-Einträge verwalten können, einschließlich der Route-53- und Verkehrsfluss-APIs. 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.
- Bei Zustandsprüfungen der Route 53 ist die Steuerebene die Route-53-Konsole und Route-53-APIs, mit denen Sie Integritätsprüfungen erstellen, aktualisieren und löschen können. 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 Amazon Route 53 Resolver besteht die Steuerebene aus der Resolver-Konsole und den APIs, mit denen Sie Amazon-VPC-Einstellungen, 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. Resolver ist ein regionaler Dienst, bei dem die 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 den Endpunkt mit einer IPv4-Adresse (192.0.2.243), einer IPv6-Adresse (2001:0db8:85a3:0000:0000:abcd:0001:2345), oder einem Domänennamen (example.com) angeben.

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

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 Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

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

Verwandte Dienstleistungen

Informationen zu den AWS Diensten, in die Amazon Route 53 integriert ist, finden Sie unterIntegration mit anderen Services.

Zugriff auf Amazon Route 53

Sie können wie folgt auf Amazon Route 53 zugreifen:

- AWS Management Console— Die Verfahren in diesem Handbuch erläutern, wie Sie mit AWS Management Console 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 die Authentifizierung, lassen sich leicht in die Entwicklungsumgebung integrieren und bieten einen 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 for Windows 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 Möglichkeit, Ihre Rechnung einzusehen und Ihr Konto und Ihre Zahlungen zu verwalten, finden Sie im AWS Billing Benutzerhandbuch.

Route 53 mit einem AWS SDK verwenden

AWS Software Development Kits (SDKs) sind für viele gängige 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 for C++	AWS SDK for C++ Code-Beispiele
AWS CLI	AWS CLI Code-Beispiele

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

Spezifische Beispiele für Route 53 finden Sie unter Codebeispiele für Route 53 unter Verwendung von 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.

Amazon Route 53 einrichten

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

Themen

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/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und 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. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer 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 Management Consoleals 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 Sie einen Benutzer 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 Benutzer in IAM Identity Center Administratorzugriff.

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

Melden Sie sich als Benutzer mit Administratorzugriff an

- 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 Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

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

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

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Tools herunterladen

Das AWS Management Console 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 Die AWS SDKs 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 der 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 for PowerShell -Cmdlet-Referenz.

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 Preisgestaltung.

Themen

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

Im Tutorial "Erste Schritte" erfahren Sie, wie Sie die folgenden Aufgaben ausführen:

- Registrieren eines Domänennamens, wie example.com
- So erstellen Sie einen Amazon-S3-Bucket und konfigurieren ihn zum Hosten einer Website

- Erstellen einer Beispiel-Website und Speichern der Datei in Ihrem S3-Bucket
- Konfigurieren von Amazon Route 53, um Datenverkehr an Ihre neue Website zu leiten

Wenn Sie fertig sind, können Sie einen Browser öffnen, den Namen der Domäne eingeben und die Website anzeigen.

> **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.

Themen

Voraussetzungen

Bevor Sie beginnen, sollten Sie sicherstellen, dass Sie die in Amazon Route 53 einrichten beschriebenen Schritte ausgeführt haben.

Schritt 1: Registrieren einer Domäne

Um einen Domänennamen wie "example.com" zu verwenden, müssen Sie einen Domänennamen suchen, der nicht bereits von einer anderen Person genutzt wird, und diesen registrieren. Sobald Sie einen Domänennamen registrieren, reservieren Sie ihn für Ihre exklusive Nutzung überall im Internet, in der Regel für ein ganzes Jahr. Standardmäßig verlängern wir den Domänennamen automatisch nach Ablauf des Jahres, aber Sie können die automatische Verlängerung auch deaktivieren. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

Schritt 2: Erstellen eines S3-Buckets für Ihre Stammdomain

Mit Amazon S3 können Sie Ihre Daten speichern und von überall aus im Internet aufrufen. Um Ihre Daten zu organisieren, erstellen Sie Buckets und laden Ihre Daten mithilfe der AWS Management Console in die Buckets hoch. Sie können mithilfe von Amazon S3 eine statische Website in einem Bucket hosten. Im folgenden Verfahren wird das Erstellen eines -Buckets erläutert.

So erstellen Sie einen S3-Bucket für www.Ihr-Domänenname

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Bucket erstellen aus.
3. Geben Sie die folgenden Werte ein:

   Bucket-Name

   Geben Sie den Namen Ihrer Domäne ein, z. B. example.com.

   Region

   Wählen Sie die Region in der Nähe der meisten Ihrer Benutzer aus.

   Notieren Sie sich die Region, die Sie auswählen. Sie benötigen diese Information zu einem späteren Zeitpunkt.
4. Um die Standardeinstellungen zu übernehmen und den Bucket zu erstellen, wählen Sie Create (Erstellen).

Schritt 3 (optional): Erstellen eines weiteren S3-Buckets für www.Ihr-Domänenname.

Im vorherigen Verfahren haben Sie einen Bucket für Ihren Domänennamen erstellt, zum Beispiel example.com. Auf diese Weise erhalten Ihre Benutzer Zugriff auf Ihre Website, indem sie den Domänennamen eingeben, zum Beispiel example.com.

Wenn Sie außerdem möchten, dass die Benutzer www.*Ihr-Domänenname* verwenden können, wie z. B. "www.example.com", um auf Ihre Beispiel-Website zuzugreifen, erstellen Sie einen zweiten S3-Bucket. Anschließend konfigurieren Sie den zweiten Bucket für die Weiterleitung des Datenverkehrs an den ersten Bucket.

So erstellen Sie einen S3-Bucket für www.Ihr-Domänenname

1. Wählen Sie Bucket erstellen aus.
2. Geben Sie die folgenden Werte ein:

   Bucket-Name

   Geben Sie www.***Ihr-Domänenname*** ein. Wenn Sie beispielsweise den Domänennamen example.com registriert haben, geben Sie www.example.com ein.

   Region

   Wählen Sie dieselbe Region aus, in der Sie den ersten Bucket erstellt haben.
3. Um die Standardeinstellungen zu übernehmen und den Bucket zu erstellen, wählen Sie Create (Erstellen).

Schritt 4: Einrichten Ihres Stammdomain-Buckets für Website-Hosting

Jetzt, da Sie einen S3-Bucket haben, können Sie ihn für Website-Hosting konfigurieren.

So erlauben Sie Website-Hosting auf Ihrem S3-Bucket

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie in der Liste Buckets den Namen des Buckets aus, für den Sie das Hosting statischer Websites aktivieren wollen.
3. Wählen Sie Properties (Eigenschaften).

4. Wählen Sie unter Static website hosting (Hosting statischer Websites) die Option Enable (Aktivieren) aus
5. Wählen Sie Use this bucket to host a website (Diesen Bucket zum Hosten einer Website verwenden).
6. Wählen Sie unter Static website hosting (Hosting statischer Websites) die Option Enable (Aktivieren) aus
7. Geben Sie unter Index document (Index-Dokument) den Dateinamen des Index-Dokuments ein, der typischerweise `index.html` ist.

   Der Name des Indexdokuments unterscheidet Groß- und Kleinschreibung und muss genau mit dem Dateinamen des HTML-Indexdokuments übereinstimmen, das Sie in den S3-Bucket hochladen möchten. Wenn Sie Ihren Bucket für das Hosting von Websites konfigurieren, müssen Sie ein Indexdokument angeben. Amazon S3 gibt dieses Indexdokument zurück, wenn Anfragen an die Root-Domäne oder einen der Unterordner gestellt werden.
8. (Optional) Wenn Sie ein eigenes benutzerdefiniertes Fehlerdokument für Fehler der Klasse 4XX bereitstellen möchten, geben Sie unter Error Document (Fehlerdokument) den Dateinamen des benutzerdefinierten Fehlerdokuments ein.

   Wenn Sie kein benutzerdefiniertes Fehlerdokument angeben und ein Fehler auftritt, wird von Amazon S3 ein Standard-HTML-Fehlerdokument zurückgegeben.
9. (Optional) Wenn Sie erweiterte Umleitungsregeln angeben möchten, geben Sie unter Redirection rules (Umleitungsregeln) XML zur Beschreibung der Regeln ein.

   Weitere Informationen finden Sie unter Konfigurieren erweiterter bedingter Weiterleitungen im Benutzerhandbuch für Amazon Simple Storage Service.
10. Wählen Sie Save Changes Änderungen speichern) aus.
11. Notieren Sie unter Static website hosting (Statisches Website-Hosting) den Wert für Endpoint (Endpunkt).

    Der Endpoint (Endpunkt) ist der Amazon-S3-Website-Endpunkt für Ihren Bucket. Nachdem Sie den Bucket als statische Website konfiguriert haben, können Sie diesen Endpunkt verwenden, um Ihre Website zu testen, wie in Schritt 9: Testen Ihres Domänen-Endpunkts zu sehen.

    Nachdem Sie die Blockierungseinstellungen für den öffentlichen Zugriff bearbeitet und eine Bucket-Richtlinie hinzugefügt haben, die öffentlichen Lesezugriff ermöglicht, können Sie den Website-Endpunkt verwenden, um auf Ihre Website zuzugreifen.

Schritt 5:(optional)Schritt: Richten Sie Ihren Subdomänen-Bucket für die Website-Umleitung ein

Nachdem Sie Ihren Stammdomain-Bucket für das Website-Hosting konfiguriert haben, können Sie Ihren Unterdomain-Bucket so konfigurieren, dass alle Anforderungen zur Stammdomain umgeleitet werden. So können Sie beispielsweise alle Anforderungen für `www.example.com`, konfigurieren, um weitergeleitet zu werden`example.com`.

So konfigurieren Sie eine Umleitung

1. Wählen Sie in der Amazon-S3-Konsole in der Liste Buckets Ihren Subdomänen-Bucket aus (in diesem Beispiel `www.example.com`).
2. Wählen Sie Properties (Eigenschaften).
3. Wählen Sie unter Static website hosting (Hosting statischer Websites) Edit (Bearbeiten) aus.
4. Wählen Sie Redirect requests for an object (Anfragen für ein Objekt umleiten).
5. Geben Sie im Feld Target bucket (Ziel-Bucket) Ihre Root-Domäne ein, z. B. **`example.com`**.
6. Wählen Sie für Protocol (Protokoll) die Option http aus.
7. Wählen Sie Save Changes (Änderungen speichern).

Schritt 6: Hochladen des Index und des Website-Inhalts

Wenn Sie das statische Website-Hosting für Ihren Bucket aktivieren, geben Sie den Namen des Indexdokuments ein (z. B, **`index.html`**). Nachdem Sie das Hosting statischer Websites für den Bucket aktiviert haben, laden Sie eine HTML-Datei mit diesem Indexdokumentnamen in Ihren Bucket hoch.

So laden Sie eine Indexdatei hoch

1. Kopieren Sie den folgenden Beispieltext, den Sie als einfache einseitige Website für dieses Lernprogramm verwenden können, fügen Sie ihn in einen Texteditor ein und speichern Sie ihn als index.html:

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

```
<body>

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

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

</body>

</html>
```

2. Wählen Sie in der Liste Buckets den Namen des Buckets aus, für den Sie das Hosting statischer Websites aktivieren wollen.
3. Wählen Sie in der Amazon-S3-Konsole den Namen des Buckets aus, den Sie im Verfahren So erlauben Sie Website-Hosting auf Ihrem S3-Bucket (auf den verknüpften Bucket-Namen klicken) erstellt haben.
4. Klicken Sie aufHochladen,Dateien hinzufügen, wählen Sie index.html aus, wo Sie sie gespeichert haben, und dannHochladenaus.
5. Wenn Sie ein Fehlerdokument erstellt haben, beispielsweise **`404.html`** führen Sie die Schritte 3 bis 5 aus, um es hochzuladen.

Schritt 7: Bearbeiten der S3 Block Public Access-Einstellungen

Standardmäßig blockiert Amazon S3 den öffentlichen Zugriff auf Ihr Konto und Ihre Buckets. Wenn Sie einen Bucket verwenden möchten, um eine statische Website zu hosten, können Sie diese Schritte verwenden, um Ihre Einstellungen für Block Public Access zu bearbeiten:

> **Warning**
>
> Bevor Sie diesen Schritt ausführen, lesen Sie den Abschnitt Verwenden von Amazon S3 Block Public Access, um sicherzustellen, dass Sie die mit dem Zulassen eines öffentlichen Zugriffs verbundenen Risiken kennen und akzeptieren. Wenn Sie die Einstellungen für Block Public Access deaktivieren, um Ihren Bucket öffentlich zu machen, kann jeder im Internet auf Ihren Bucket zugreifen. Wir empfehlen Ihnen, den gesamten öffentlichen Zugriff auf Ihre Buckets zu blockieren.

So leiten Sie den Datenverkehr an Ihre Website

1. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, den Sie als statische Website konfiguriert haben.
3. Wählen Sie Permissions (Berechtigungen).
4. Wählen Sie unter Block public access (bucket settings) (Öffentlichen Zugriff blockieren (Bucket-Einstellungen)), die Option Edit (Bearbeiten).
5. Löschen Sie Block all public access (Gesamten öffentlichen Zugriff blockieren) und wählen Sie Save changes (Änderungen speichern).

Amazon S3 deaktiviert die Block Public Access-Einstellungen für Ihren Bucket. Um eine öffentliche, statische Website zu erstellen, müssen Sie möglicherweise auch die Block Public Access-Einstellungen für Ihr Konto bearbeiten, bevor Sie eine Bucket-Richtlinie hinzufügen. Wenn Kontoeinstellungen für Block Public Access derzeit aktiviert sind, wird unter Block public access (bucket settings) (Öffentlichen Zugriff blockieren (Bucket-Einstellungen)) ein Hinweis angezeigt.

Schritt 8: Anfügen einer Bucket-Richtlinie

Nachdem Sie die Einstellungen für Amazon S3 Block Public Access bearbeitet haben, können Sie eine Bucket-Richtlinie hinzufügen, um öffentlichen Lesezugriff auf Ihre Bucket-Objekte zu gewähren. Wenn Sie öffentlichen Lesezugriff gewähren, kann jeder im Internet auf Ihren Bucket zugreifen.

> **Warning**
>
> Bevor Sie diesen Schritt ausführen, lesen Sie den Abschnitt Verwenden von Amazon S3 Block Public Access, um sicherzustellen, dass Sie die mit dem Zulassen eines öffentlichen Zugriffs verbundenen Risiken kennen und akzeptieren. Wenn Sie die Einstellungen für Block Public Access deaktivieren, um Ihren Bucket öffentlich zu machen, kann jeder im Internet auf Ihren Bucket zugreifen. Wir empfehlen Ihnen, den gesamten öffentlichen Zugriff auf Ihre Buckets zu blockieren.

So leiten Sie den Datenverkehr an Ihre Website

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie unter Buckets den Namen Ihres Buckets aus.
3. Wählen Sie Permissions (Berechtigungen).

4. Wählen Sie unter Bucket Policy (Bucket-Richtlinie) Edit (Bearbeiten).
5. Kopieren Sie die folgende Bucket-Richtlinie, und fügen Sie sie in einen Texteditor ein. Diese Richtlinie gewährt jedem Benutzer im Internet (`"Principal":"*"`) die Berechtigung, die Dateien (`"Action":["s3:GetObject"]`) im S3-Bucket abzurufen, der Ihrem Domänennamen (`"arn:aws:s3:::`*`your-domain-name`*`/*"`) zugeordnet ist:

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

6. Aktualisieren des Werts für `Resource` auf *`Ihr-Domänenname`*, zum Beispiel **`example.com`**.
7. Wählen Sie Änderungen speichern aus.

Schritt 9: Testen Ihres Domänen-Endpunkts

Nachdem Sie den Stammdomain-Bucket zum Hosten einer öffentlichen Website konfiguriert haben, können Sie Ihren Endpunkt testen. Sie können nur den Endpunkt für Ihren Domänen-Bucket testen, da Ihr Subdomänen-Bucket für die Website-Umleitung und nicht für das statische Website-Hosting eingerichtet ist.

> **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 HTTPS für die Kommunikation zwischen Zuschauern erforderlich machen und CloudFront.

1. Wählen Sie unter Buckets den Namen Ihres Buckets aus.
2. Wählen Sie Properties (Eigenschaften).
3. Wählen Sie unten auf der Seite unter Static website hosting (Hosting statischer Websites) Ihren Bucket-Website-Endpunkt.

   Ihr Indexdokument wird in einem separaten Browserfenster geöffnet.

Schritt 10: Weiterleiten von DNS-Datenverkehr für Ihre Domäne an den Website-Bucket

Sie verfügen jetzt über eine einseitige Website in Ihrem S3-Bucket. Um den Internetdatenverkehr für Ihre Domäne an Ihren S3-Bucket weiterzuleiten, führen Sie die folgenden Schritte durch.

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).

   > **Note**
   >
   > Jeder Datensatz enthält Informationen darüber, wie Sie den Datenverkehr für eine Domäne (z. B. example.com) oder eine Subdomäne (z. B. www.example.com oder test.example.com) weiterleiten wollen. Datensätze werden in der gehosteten Zone für Ihre Domäne gespeichert.

5. Wählen Sie Switch to wizard (Zu Assistent wechseln) aus.
6. Wählen Sie Simple Routing (Einfaches Routing), und wählen Sie Next (Weiter).
7. Wählen Sie Define simple record (Einfachen Datensatz definieren).

8. Akzeptieren Sie unter Record name (Datensatzname) den Standardwert, bei dem es sich um den Namen Ihrer gehosteten Zone und Ihrer Domäne handelt.
9. Wählen Sie unter Datensatztyp die Option A - Leitet den Datenverkehr an eine IPv4-Adresse und einige AWS Ressourcen weiter.
10. Wählen Sie unter Value/Route traffic to (Wert/Datenverkehr weiterleiten zu) die Option Alias to S3 website endpoint (Alias zu S3-Website-Endpunkt) aus.
11. Wählen Sie die Region aus.
12. Wählen Sie den S3-Bucket.

    Der Bucket-Name sollte mit dem Namen übereinstimmen, der im Feld Name angezeigt wird. In der Liste Choose S3 Bucket (S3-Bucket auswählen) wird der Bucket-Name mit dem Amazon-S3-Website-Endpunkt für die Region angezeigt, in der der Bucket erstellt wurde, zum Beispiel `s3-website-us-west-1.amazonaws.com (example.com)`.

    Wählen Sie den S3-BucketListet einen Bucket auf, wenn einer der folgenden Bedingungen erfüllt ist:

    - Sie den Bucket als statische Website konfiguriert haben.
    - Der Name des Buckets mit dem Namen des Datensatzes übereinstimmt, den Sie anlegen.
    - Das AWS Girokonto hat den Bucket erstellt.

    Wenn Ihr Bucket nicht in der Auflistung Choose S3 bucket (S3-Bucket auswählen) angezeigt wird, geben Sie den Amazon-S3-Website-Endpunkt für die Region ein, in der der Bucket erstellt wurde, z. B. **`s3-website-us-west-2.amazonaws.com`**. Eine vollständige Liste der Amazon-S3-Website-Endpunkte finden Sie unter Amazon-S3-Website-Endpunkte. Weitere Informationen über das Alias-Target finden Sie im Abschnitt „Wert/Datenverkehr weiterleiten zu“ unterSpezifische Werte für einfache Aliasdatensätzeaus.
13. Wählen Sie unter Evaluate target health (Zielzustand bewerten) die Option No (Nein).
14. Wählen Sie Define simple record (Einfachen Datensatz definieren).

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 unter Configure records (Datensätze konfigurieren) die Option Define simple record (Einfachen Datensatz definieren) aus
2. Geben Sie unter Record name (Datensatzname) für Ihre Subdomäne `www` ein.
3. Wählen Sie unter Datensatztyp die Option A - Leitet den Datenverkehr an eine IPv4-Adresse und einige AWS Ressourcen weiter.
4. Wählen Sie unter Value/Route traffic to (Wert/Datenverkehr weiterleiten zu) die Option Alias to S3 website endpoint (Alias zu S3-Website-Endpunkt) aus.
5. Wählen Sie die Region aus.
6. Wählen Sie den S3-Bucket, zum Beispiel, `s3-website-us-west-2.amazonaws.com (example.com)`.

   Wenn Ihr Bucket nicht in der Auflistung Choose S3 bucket (S3-Bucket auswählen) angezeigt wird, geben Sie den Amazon-S3-Website-Endpunkt für die Region ein, in der der Bucket erstellt wurde, z. B. **`s3-website-us-west-2.amazonaws.com`**.
7. Wählen Sie unter Evaluate target health (Zielzustand bewerten) die Option No (Nein).
8. Wählen Sie Define simple record (Einfachen Datensatz definieren).
9. Klicken Sie auf der Seite Configure records (Datensätze konfigurieren) auf Create records (Datensätze erstellen).

Schritt 11: Testen Ihrer Website

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

- http://*`Ihr-Domänenname`* `example.com` Zeigt das Indexdokument im Bucket *`Ihr-Domänenname`* an.
- http://www.*`Ihr-Domänenname`* `www.example.com` Leitet Ihre Anfrage an den Bucket *`Ihr-Domänenname`* 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.

Schritt 12 (optional): Verwenden Sie Amazon CloudFront , um die Verbreitung Ihrer Inhalte zu beschleunigen

CloudFront ist ein Webservice, der die Verteilung Ihrer statischen und dynamischen Webinhalte wie .html-, .css-, .js- und Bilddateien an Ihre Benutzer beschleunigt. CloudFront stellt Ihre Inhalte über ein weltweites Netzwerk von Rechenzentren bereit, die als Edge-Standorte bezeichnet werden. Wenn ein Benutzer Inhalte anfordert CloudFront, mit denen Sie sie bereitstellen, wird der Benutzer an den Edge-Standort weitergeleitet, der die niedrigste Latenz (Zeitverzögerung) bietet, sodass der Inhalt mit der bestmöglichen Leistung bereitgestellt wird.

- Wenn sich der Inhalt bereits am Edge-Standort mit der geringsten Latenz befindet, wird CloudFront er sofort bereitgestellt.
- Wenn sich der Inhalt nicht an diesem Edge-Standort befindet, CloudFront ruft er ihn von einem Amazon S3 S3-Bucket oder einem HTTP-Server (z. B. einem Webserver) ab, den Sie als Quelle für die endgültige Version Ihres Inhalts identifiziert haben.

Informationen zur Verwendung CloudFront zur Verteilung der Inhalte in Ihrem Amazon S3-Bucket finden Sie unter Hinzufügen, CloudFront wenn Sie Inhalte von Amazon S3 verteilen im Amazon CloudFront Developer Guide.

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

Im Tutorial "Erste Schritte" erfahren Sie, wie Sie die folgenden Aufgaben ausführen:

- Registrieren eines Domänennamens, wie example.com
- Erstellen Sie ein Zertifikat für Ihre Domäne.
- Erstellen Sie zwei Amazon S3 Buckets, und konfigurieren Sie einen für das Hosten einer Website und den anderen für die Umleitung zur Subdomain.
- Erstellen einer Beispiel-Website und Speichern der Datei in Ihrem S3-Bucket
- Erstellen Sie CloudFront Distributionen für beide S3-Buckets.
- Konfigurieren Sie Amazon Route 53 so, dass der Verkehr zu den CloudFront Distributionen weitergeleitet wird.

Wenn Sie fertig sind, können Sie einen Browser öffnen, den Namen der Domäne eingeben und die Website anzeigen.

Themen

Voraussetzungen

Bevor Sie beginnen, sollten Sie sicherstellen, dass Sie die in Amazon Route 53 einrichten beschriebenen Schritte ausgeführt haben.

Schritt 1: Registrieren einer Domäne

Um einen Domänennamen wie "example.com" zu verwenden, müssen Sie einen Domänennamen suchen, der nicht bereits von einer anderen Person genutzt wird, und diesen registrieren. Sobald Sie einen Domänennamen registrieren, reservieren Sie ihn für Ihre exklusive Nutzung überall im Internet, in der Regel für ein ganzes Jahr. Standardmäßig wird der Domainname automatisch am Jahresende verlängert. Die automatische Verlängerung kann aber auch deaktiviert werden. Weitere Informationen finden Sie unter Registrieren einer neuen Domain.

Schritt 2: Anfordern eines öffentlichen Zertifikats

Für die Konfiguration Ihrer CloudFront Amazon-Distributionen ist ein öffentliches Zertifikat erforderlich, sodass Zuschauer HTTPS verwenden CloudFront müssen, sodass Verbindungen bei der CloudFront Kommunikation mit Zuschauern verschlüsselt werden.

Um ein öffentliches AWS Certificate Manager(ACM-) Zertifikat anzufordern (Konsole)

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die ACM-Konsole unter https://console.aws.amazon.com/acm/home.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie das Zertifikat in der Region USA Ost (Nord-Virginia) anfordern oder importieren (). Dies ist für Amazon erforderlich CloudFront.

   Wählen Sie im linken Navigationsbereich die Option Zertifikat anfordern und auf der Seite Zertifikat anfordern die Option Öffentliches Zertifikat anfordern und dann Weiter aus.
2. Geben Sie im Abschnitt Domainnamen Ihre Domain ein, z. B. **`example.com`**.

   Wählen Sie Fügen Sie diesem Zertifikat einen weiteren Namen hinzu aus und geben Sie ein Sternchen vor dem Domainnamen ein, um ein Platzhalterzertifikat für alle Unterdomains anzufordern, z. B. **`*.example.com`**.
3. Wählen Sie im Abschnitt Validierungsmethode auswählen die Option DNS-Validierung aus.
4. Wählen Sie im Abschnitt Schlüsselalgorithmus die Option RSA 2048 aus.
5. Im Abschnitt Tags hinzufügen können Sie Ihr Zertifikat optional mit Tags versehen. Tags sind Schlüssel-Wert-Paare, die als Metadaten zur Identifizierung und Organisation AWS von Ressourcen dienen.

   Wählen Sie Abfrage aus, um zur Seite Zertifikate zu gelangen.
6. Wenn Ihr neues Zertifikat den Status Ausstehend hat, wählen Sie die Zertifikat-ID und auf der Seite mit den Zertifikatdetails die Option Eintrag in Route 53 erstellen aus, um die CNAME-Einträge für Ihre Domains automatisch hinzuzufügen. Wählen Sie anschließend Einträge erstellen aus.

   Die Seite Certificate status (Zertifikatstatus) sollte mit einem Statusbanner geöffnet werden, das die Meldung Successfully created DNS records (DNS-Einträge erfolgreich erstellt) enthält.

   Ihr neues Zertifikat kann noch bis zu 30 Minuten lang den Status Pending validation (Validierung ausstehend) anzeigen.

Schritt 3: Erstellen eines S3-Buckets zum Hosten Ihrer Subdomäne

So erstellen Sie einen S3-Bucket für www.Ihr-Domänenname

Mit Amazon S3 können Sie Ihre Daten speichern und von überall aus im Internet aufrufen. In diesem Schritt erstellen Sie einen S3-Bucket, um alle Dateien für Ihre Website zu speichern.

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Bucket erstellen aus.
3. Geben Sie die folgenden Werte ein:

   Bucket-Name

   Geben Sie www.***Ihr-Domänenname*** ein. Wenn Sie beispielsweise den Domänennamen example.com registriert haben, geben Sie www.example.com ein.

   Region

   Wählen Sie eine Region für Ihren Bucket aus.
4. Um die Standardeinstellungen zu übernehmen und den Bucket zu erstellen, wählen Sie Create (Erstellen).

   Weitere Informationen zu S3-Bucket-Einstellungen finden Sie unter View bucket properties (Anzeigen von Bucket-Eigenschaften) im Amazon S3 Benutzerhandbuch.

Schritt 4: Erstellen eines weiteren S3-Buckets für Ihre Stammdomain

Wenn Sie außerdem möchten, dass die Benutzer *.your-domain-name* verwenden können (wie z. B. example.com), um auf Ihre Beispiel-Website zuzugreifen, erstellen Sie einen zweiten S3-Bucket. In diesem Tutorial konfigurieren Sie dann den zweiten Bucket (Stammdomain) für die Weiterleitung des Datenverkehrs an den ersten Bucket.

So erstellen Sie einen S3-Bucket für www.Ihr-Domänenname

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Bucket erstellen aus.
3. Geben Sie die folgenden Werte ein:

Bucket-Name

Geben Sie ***your-domain-name*** ein. Wenn Sie beispielsweise den Domänennamen example.com registriert haben, geben Sie www.example.com ein.

Region

Wählen Sie dieselbe Region aus, in der Sie den ersten Bucket erstellt haben.

4. Um die Standardeinstellungen zu übernehmen und den Bucket zu erstellen, wählen Sie Create (Erstellen).

Schritt 5: Hochladen von Website-Dateien in Ihren Subdomain-Bucket

Nachdem Sie nun einen S3-Bucket haben, können Sie Ihre Website-Dateien hochladen. In diesem Tutorial laden Sie lediglich eine einfache Datei vom Typ „index.html“ hoch, die Text auf einer Seite anzeigt.

So aktivieren Sie das Website-Hosting für einen S3-Bucket:

1. Öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie in der Liste Buckets den verknüpften Namen des Buckets aus, in den die Website-Dateien hochgeladen werden sollen z. B.**www.example.com**.
3. Kopieren Sie den Beispieltext, der eine einfache einseitige Webseite erstellt, fügen Sie ihn in einen Texteditor ein und speichern Sie ihn als index.html:

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

<body>

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

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

```
</body>

</html>
```

4. Wählen Sie auf der Registerkarte Objekte die Option Hochladen aus.
5. Wählen Sie unter Files and folders (Dateien und Ordner) Add files (Dateien hinzufügen)aus und laden Sie Ihre Website-Dateien hoch. Laden Sie für dieses Tutorial die Datei index.html hoch, die Sie in Schritt 3 dieses Verfahrens gespeichert haben.

Schritt 6: Einrichten Ihres Stammdomain-Buckets für die Website-Umleitung

Nachdem Sie Ihren Stammdomain-Bucket für das Website-Hosting konfiguriert haben, können Sie Ihren Stammdomain-Bucket so konfigurieren, dass alle Anforderungen an die Unterdomain umgeleitet werden. So können Sie beispielsweise alle Anforderungen für `example.com`, konfigurieren, um weitergeleitet zu werden`www.example.com`.

So konfigurieren Sie eine Umleitung

1. Wählen Sie in der Amazon-S3-Konsole in der Liste Buckets Ihren Subdomänen-Bucket aus (in diesem Beispiel `example.com`).
2. Wählen Sie Properties (Eigenschaften).
3. Wählen Sie unter Static website hosting (Hosting statischer Websites) Edit (Bearbeiten) aus.
4. Wählen Sie unter Static website hosting (Hosting statischer Websites) die Option Enable (Aktivieren) aus
5. Wählen Sie Redirect requests for an object (Anfragen für ein Objekt umleiten).
6. Geben Sie in Host name (Hostname) Ihre Subdomain ein, z. B.**`www.example.com`**.
7. Wählen Sie für Protocol (Protokoll) die Option HTTPS aus.
8. Wählen Sie Save Changes Änderungen speichern) aus.
9. Notieren Sie unter Static website hosting (Statisches Website-Hosting) den Wert für Endpoint (Endpunkt).

   Der Endpoint (Endpunkt) ist der Amazon-S3-Website-Endpunkt für Ihren Bucket. Sie werden diesen Endpunkt verwenden, um eine CloudFront Amazon-Distribution einzurichten.

Schritt 7: Erstellen Sie eine CloudFront Amazon-Distribution für Ihre Subdomain

In diesem Schritt erstellen Sie eine CloudFront Distribution für Ihre Subdomain, z. B. www.example.com, damit Ihre Website HTTPS verwenden kann, sodass die Benutzer sie sicher aufrufen können.

Erstellen Sie CloudFront-Verteilungen wie folgt:

1. Öffnen Sie die Konsole unter CloudFront . https://console.aws.amazon.com/cloudfront/v4/home
2. Wählen Sie Create Distribution (Distribution erstellen).
3. Wählen Sie unter Ursprung für Ursprungsdomain den Amazon-S3-Bucket aus, den Sie zuvor erstellt haben. Das Format wird ähnlich aussehen wie**`www.example.com.s3.<Region>.amazonaws.com`**.

   Wählen Sie für Ursprungszugriff die Option Legacy-Zugriffsidentitäten aus. Wählen Sie aus der Liste Origin access identity (Ursprungszugriffsidentität) aus oder wählen SieCreate new OAI (Neues OAI erstellen)(beide funktionieren) aus.

   Wählen Sie für Bucket policy (Bucket-Richtlinie)Yes, update the bucket policy (Ja, aktualisieren Sie die Bucket-Richtlinie) aus.
4. Für die Einstellungen unter Einstellungen für das Cache-Verhalten, unterViewer setzen Sie Betrachter-Protokollrichtlinien auf HTTP nach HTTPS umleiten und übernehmen Sie für den Rest die Standardwerte.

   Weitere Informationen zu den Optionen für das Cache-Verhalten finden Sie unter Einstellungen für das Cache-Verhalten im CloudFront Amazon-Entwicklerhandbuch.
5. Im Abschnitt Webanwendungsfirewall (WAF) können Sie AWS WAF -Sicherheitsvorkehrungen aktivieren oder deaktivieren.
6. Für die Felder unterEinstellungenwie folgt:

   - Wählen Sie Add item (Element hinzufügen) für Alternate domain name (CNAME) - optional (Alternativer Domain-Name (CNAME) - optional) aus und geben Sie Ihre Subdomain ein, z. B. **`www.example.com`**.
   - Wählen Sie für Custom SSL Certificate (Benutzerdefiniertes SSL-Zertifikat) das Zertifikat aus, das Sie zuvor erstellt haben.
   - Geben Sie in das Textfeld Default root object (Standardstammobjekt) **`index.html`** ein.

- Behalten Sie ansonsten die Standardwerte bei und wählen Sie Distribution erstellen aus.

  Weitere Informationen zu Verteilungsoptionen finden Sie unter Distribution Settings (Einstellungen für die Verteilung).

7. Nachdem Sie Ihre Verteilung CloudFront erstellt haben, ändert sich der Wert der Spalte Status für Ihre Verteilung von In Bearbeitung zu Bereitgestellt. Dies dauert in der Regel einige Minuten.

   Notieren Sie sich den Domainnamen, der Ihrer Distribution CloudFront zugewiesen wurde und der in der Liste der Distributionen angezeigt wird. Sie können diesen Domänennamen verwenden, um die Verteilung zu testen.

Schritt 8: Erstellen Sie eine CloudFront Amazon-Distribution für Ihre Root-Domain

In diesem Schritt erstellen Sie eine CloudFront Distribution für Ihre Root-Domain, sodass sie HTTPS verwendet, wenn ihre URL zur Subdomain umgeleitet wird.

Erstellen Sie CloudFront-Verteilungen wie folgt:

1. Öffnen Sie die CloudFront Konsole unter. https://console.aws.amazon.com/cloudfront/v4/home
2. Wählen Sie Create Distribution (Verteilung erstellen).
3. Geben Sie unter Origin Settings (Ursprüngliche Einstellungen) für Origin Domain Name (Ursprünglicher Domänenname) den Endpunkt der Bucket-Website ein. Sie erhalten dies aus dem Abschnitt Static website hosting (Hosten statischer Websites) der Properties (Eigenschaften) für den Amazon S3 Bucket, den Sie zuvor erstellt haben.

   Übernehmen Sie für den Rest die Standardwerte.
4. Im Abschnitt Webanwendungsfirewall (WAF) können Sie AWS WAF -Sicherheitsvorkehrungen aktivieren oder deaktivieren.
5. Wählen Sie für die Felder unter Cache-Schlüssel und Quellanforderungen die Option Cache-Richtlinie und Richtlinie für ursprüngliche Anfragen (empfohlen) aus und wählen Sie im Drop-down-Menü Cache-Richtlinie die Option CachingDisabled

   Übernehmen Sie für den Rest die Standardwerte.

Weitere Informationen zu den Optionen für das Cache-Verhalten finden Sie unter Einstellungen für das Cache-Verhalten im CloudFront Amazon-Entwicklerhandbuch.

6. Für die Felder unterEinstellungenwie folgt:

   - Wählen Sie Add item (Element hinzufügen) für Alternate domain name (CNAME) - optional (Alternativer Domain-Name (CNAME) - optional) aus, und geben Sie Ihre Stammdomäne ein, z. B. **`example.com`** ein.
   - Wählen Sie für Benutzerdefiniertes SSL-Zertifikat das Zertifikat aus, das Sie zuvor erstellt haben.
   - Übernehmen Sie für den Rest die Standardwerte.

   Weitere Informationen zu Verteilungsoptionen finden Sie unter Distribution Settings (Einstellungen für die Verteilung).

7. Klicken Sie unten auf der Seite auf Create Distribution (Verteilung erstellen).
8. Nachdem Sie Ihre Verteilung CloudFront erstellt haben, ändert sich der Wert der Spalte Status für Ihre Verteilung von In Bearbeitung zu Bereitgestellt. Dies dauert in der Regel einige Minuten.

   Notieren Sie sich den Domainnamen, der Ihrer Distribution CloudFront zugewiesen wurde und der in der Liste der Distributionen angezeigt wird. Sie können diesen Domänennamen verwenden, um die Verteilung zu testen,

Schritt 9: Leiten Sie den DNS-Verkehr für Ihre Domain an Ihre Distribution weiter CloudFront

Sie haben jetzt eine einseitige Website in Ihrem S3-Bucket, die eine CloudFront Distribution verwendet. Gehen Sie wie folgt vor, um mit der Weiterleitung des Internetverkehrs für Ihre Domain an die CloudFront Distribution zu beginnen.

Weitere Informationen zur Weiterleitung von Datenverkehr 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).

   Wenn Sie sich in der Ansicht Quick create record (Rekord schnell erstellen) wählen Sie Switch to wizard (Zu Assistent wechseln) aus.

   > **Note**
   >
   > Jeder Datensatz enthält Informationen darüber, wie Sie den Datenverkehr für eine Domäne (z. B. example.com) oder eine Subdomäne (z. B. www.example.com oder test.example.com) weiterleiten wollen. Datensätze werden in der gehosteten Zone für Ihre Domäne gespeichert.

5. Wählen Sie Simple Routing (Einfaches Routing), und wählen Sie Next (Weiter).
6. Wählen Sie Define simple record (Einfachen Datensatz definieren).
7. Akzeptieren Sie unter Record name (Datensatzname) **www** vor dem Standardwert, bei dem es sich um den Namen Ihrer gehosteten Zone und Ihrer Domäne handelt.
8. Wählen Sie unter Datensatztyp die Option A - Leitet den Datenverkehr an eine IPv4-Adresse und einige AWS Ressourcen weiter.
9. Wählen Sie unter Value/Traffic weiterleiten an die Option Alias to Distribution aus. CloudFront
10. Wählen Sie Verteilung erstellen.

    Der Verteilungsname muss mit dem Namen übereinstimmen, der im Feld Domain name (Domänenname) in der Liste Distributions (Verteilungen) angezeigt wird, z. B. `dddjjjkkk.cloudfront.net`.
11. Wählen Sie unter Evaluate target health (Zielzustand bewerten) die Option No (Nein).
12. Wählen Sie Define simple record (Einfachen Datensatz definieren).

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

Fügen Sie auch einen Aliasdatensatz für Ihre Stammdomäne hinzu, sodass er auf den S3-Bucket verweist, der den Datenverkehr an `www.example.com` umleitet. Weitere Informationen zur Weiterleitung von Datenverkehr an CloudFront Verteilungen finden Sie unter. Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens

1. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
2. Wählen Sie in der Liste der gehosteten Zonen den Namen Ihrer Domäne aus.
3. Wählen Sie Create record (Datensatz erstellen).

   Wenn Sie sich in der Ansicht Quick create record (Rekord schnell erstellen) wählen Sie Switch to wizard (Zu Assistent wechseln) aus.

   > **Note**
   >
   > Jeder Datensatz enthält Informationen darüber, wie Sie den Datenverkehr für eine Domäne (z. B. example.com) oder eine Subdomäne (z. B. www.example.com oder test.example.com) weiterleiten wollen. Datensätze werden in der gehosteten Zone für Ihre Domäne gespeichert.

4. Wählen Sie Simple Routing (Einfaches Routing), und wählen Sie Next (Weiter).
5. Wählen Sie Define simple record (Einfachen Datensatz definieren).
6. In Record name (Datensatzname) übernehmen Sie den Standardwert.
7. Wählen Sie unter Datensatztyp die Option A - Leitet den Datenverkehr an eine IPv4-Adresse und einige AWS Ressourcen weiter.
8. Wählen Sie unter Value/Traffic weiterleiten an die Option Alias to Distribution aus. CloudFront
9. Wählen Sie Verteilung erstellen.

   Der Verteilungsname muss mit dem Namen übereinstimmen, der im Feld Domain name (Domänenname) in der Liste Distributions (Verteilungen) angezeigt wird, z. B. `dddjjjkkk.cloudfront.net`.
10. Wählen Sie unter Evaluate target health (Zielzustand bewerten) die Option No (Nein).
11. Wählen Sie Define simple record (Einfachen Datensatz definieren).
12. Klicken Sie auf der Seite Configure records (Datensätze konfigurieren) auf Create records (Datensätze erstellen).

Schritt 10: Testen Ihrer Website

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

- http://*Ihr-Domänenname* beispielsweise `www.example.com` zeigt das Indexdokument im Bucket *Ihr-Domänenname* an.
- http://www.*Ihr-Domänenname* `example.com` Leitet Ihre Anfrage an den Bucket *Ihr-Domänenname* 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. Informationen zur Weiterleitung Ihres Internetverkehrs zu AWS Ressourcen finden Sie unter. Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen

Integration mit anderen Services

Sie können Amazon Route 53 in andere AWS-Services integrieren, um die Anforderungen 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 in AWS CloudTrail integriert, einem Service, der Informationen über jede Anforderung erfasst, die von Ihrem AWS-Konto an die Route 53-API gesendet wird. Anhand der in den CloudTrail-Protokolldateien erfassten Informationen können Sie unter anderem die Anforderung an Route 53, die Quell-IP-Adresse, von der die Anforderung ausging, den Ersteller sowie den Erstellungszeitpunkt der Anforderung ermitteln.

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

Amazon CloudWatch

Sie können Amazon CloudWatch verwenden, um den Status Ihrer Route 53-Zustandsprüfungen — gesund oder ungesund — 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 Markierung, die Sie einer AWS-Ressource zuweisen, wie Route 53-Domänen, gehostete Zonen sowie Zustandsprüfungen. Jedes Tag besteht aus einem Schlüssel und

einem Wert, die Sie beide selbst definieren können. Beispielsweise können Sie ein Tag zu einer Domänenregistrierung zuweisen, die den Schlüssel "Kunde" und den Wert "Beispielfirma" hat. Sie können Tags für verschiedene Zwecke nutzen; eine häufige Nutzung ist die Kategorisierung und Nachverfolgung der AWS-Kosten.

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

Weiterleiten des Datenverkehrs an andere AWS-Ressourcen

Sie können mithilfe von Amazon Route 53 Datenverkehr an verschiedene AWS-Ressourcen weiterleiten.

Amazon API Gateway

Mit Amazon API Gateway können Sie APIs in jedem Umfang erstellen, veröffentlichen, warten, überwachen und sichern. Sie können APIs erstellen, die auf AWS oder andere Web-Services sowie auf Daten zugreifen können, die in der AWS Cloud gespeichert sind.

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 von Web-Inhalten zu beschleunigen, können Sie Amazon CloudFront verwenden, das AWS-Netzwerk zur Bereitstellung von Inhalten (Content Delivery Network, CDN). CloudFront ermöglicht die Bereitstellung Ihrer gesamten Website, einschließlich dynamischer, statischer, gestreamter und interaktiver Inhalte, mithilfe eines globalen Netzwerks von Edge-Standorten. CloudFront leitet Anforderungen für Ihre Inhalte an den Edge-Standort, der die niedrigste Latenz für Ihre Benutzer aufweist. Sie können mithilfe von Route 53 den Datenverkehr für Ihre Domäne an die CloudFront-Verteilung weiterleiten. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

Amazon EC2

Amazon EC2 stellt skalierbare Rechenkapazität in der AWS Cloud bereit. Sie können eine virtuelle EC2-Rechenumgebung (eine Instance) mithilfe einer vorkonfigurierten Vorlage (einem Amazon Machine Image oder AMI) starten. Wenn Sie eine EC2-Instance starten, installiert EC2 automatisch das Betriebssystem (Linux oder Microsoft Windows) und zusätzliche Software aus dem AMI, wie z. B. Webserver oder Datenbanksoftware.

Wenn Sie eine Website hosten oder eine Webanwendung auf einer EC2-Instance ausführen, können Sie den Datenverkehr für Ihre Domäne, wie beispielsweise "beispiel.com", mithilfe von Route 53 an Ihren Server weiterleiten. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs an eine Amazon-EC2-Instance.

AWS Elastic Beanstalk

Wenn Sie AWS Elastic Beanstalk für die Bereitstellung und Verwaltung von Anwendungen in der AWS-Cloud verwenden, können Sie mithilfe von Route 53 DNS-Datenverkehr für Ihre Domäne, wie "beispiel.com", an eine Elastic Beanstalk-Umgebung weiterleiten. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs in eine AWS Elastic Beanstalk Umgebung.

Elastic Load Balancing

Wenn Sie eine Website auf mehreren Amazon-EC2-Instances hosten, können Sie den Datenverkehr auf Ihrer Website mithilfe eines Elastic Load Balancers (ELB) an alle 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)

Ein Schnittstellenendpunkt ermöglicht die Verbindung zu Services, die von AWS PrivateLink unterstützt werden. Zu diesen Services gehören verschiedene AWS-Services, die von anderen AWS-Kunden und -Partnern in ihren eigenen VPCs gehostet werden (auch als Endpunktservices bezeichnet), sowie unterstützte AWS Marketplace-Partnerservices.

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 Unternehmen-E-Mails nutzen und Sie Route 53 als DNS-Service verwenden, können Sie mit Datenverkehr an Ihre Amazon WorkMail E-Mail-Domäne weiterleiten. 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.

Themen

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.

Enthält Ihr Domänenname eines der folgenden Zeichen, müssen Sie die Zeichen durch Escape-Zeichen im Format *dreistelliger Oktalcode* angeben:

- 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).
- 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 Domänennamen (IDNs) als Punycode, der Unicode-Zeichen als ASCII-Zeichenfolgen 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) IDNs und die Sprache unterstützt, die Sie verwenden möchten. 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 IDNs oder die Sprache, die Sie für Ihren Domänennamen verwenden möchten, 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 eines der AWS SDKs verwenden, 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.

Beachten Sie bei der Registrierung eines Domänenamens, dass nicht alle Top-Level-Domänen (TLDs) IDNs unterstützen. Sie finden eine Liste der von Route 53 unterstützten TLDs unter Domains, die Sie mit Amazon Route 53 registrieren können. Es werden die TLDs angegeben, die IDNs nicht unterstützen.

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 die APIs zu arbeiten. Die SDKs vereinfachen die Authentifizierung, lassen sich leicht in die Entwicklungsumgebung integrieren und bieten einen einfachen Zugriff auf die Befehle von Route 53.

Domainnamen-Registrierungsservices werden gemäß der Domainnamen-Registrierungsvereinbarung bereitgestellt.

Themen

- Übertragung des Registrars an Amazon Registrar
- Erneutes Senden von Autorisierungs- und Bestätigungs-E-Mails
- 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

Informationen zum Registrieren und Übertragen neuer Domains sowie zum Anzeigen des Domainregistrierungsstatus finden Sie im jeweiligen Thema.

Themen

- Registrieren einer neuen Domain
- Angegebene Werte beim Registrieren oder Übertragen einer Domain
- Von Amazon Route 53 zurückgegebene Werte beim Registrieren einer Domain
- Anzeigen des Status einer Domainregistrierung

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 finden Sie unter Domains, 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 Verkehr für Ihre Domain weiterleiten, z. B. an eine Amazon EC2 EC2-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 Route 53-Konsole unter https://console.aws.amazon.com/route53/ an AWS Management Console und öffnen Sie sie.
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.

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

Bei einigen Domains oberster Ebene (Top-Level-Domains, TLDs) müssen wir weitere Informationen erfassen. Geben Sie für diese TLDs die entsprechenden Werte hinter dem Feld Postal/Zip Code (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. Nur Kunden von AISPL (Indien): Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen Verkäufer in Indien. AWS Um eine Domain bei Route 53 zu registrieren, führen Sie die folgenden Schritte aus, um die Gebühr für die Registrierung Ihrer Domain zu bezahlen.

   a. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.

   b. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.

   c. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

      Nachdem Sie die Rechnung bezahlt haben, schließen wir die Domainregistrierung ab und senden die entsprechenden E-Mails.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um eine Domain zu registrieren, nachdem eine Rechnung storniert wurde, übermitteln Sie die Anforderung erneut.

Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

9. 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.com – Für TLDs, die von der Amazon-Vergabestelle registriert wurden.
   - noreply@domainnameverification.net Für TLDs, die von unserem Registrierungspartner Gandi registriert wurden. 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.

10. 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.
- Bei einigen TLDs hängt der verfügbare Datenschutz vom ausgewählten Contact Type ab. 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 First Name (Vorname) und/oder Last Name (Nachname) für den Registranten-Kontakt aus 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
Von Amazon Registrar registrierte TLDs	noreply@registrar.amazon.com
.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

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
Von Amazon Registrar registrierte TLDs	noreply@registrar.amazon.com
.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

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 eingeben:

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

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

Außerdem erfordern viele TLDs 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).

Der Registrierungszeitraum beträgt in der Regel ein Jahr, wobei 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.

Für die meisten TLDs können Sie den Registrierungszeitraum auf 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..

Namensserver

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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

Weitere Informationen zum Aktualisieren von Einstellungen für eine Domäne finden Sie unter den entsprechenden Themen.

Themen

- Aktualisieren der Kontaktinformationen und des Eigentümers einer Domäne
- Aktivieren oder Deaktivieren des Datenschutzes für Kontaktinformationen für eine Domäne
- Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domäne
- Sperren einer Domäne zum Verhindern der nicht autorisierten Übertragung an eine andere Vergabestelle
- Verlängern des Registrierungszeitraums für eine Domäne
- Aktualisieren von Namenservern für die Verwendung einer anderen Vergabestelle
- Hinzufügen oder Ändern der Nameserver und Glue-Datensätze in einer Domäne

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 muss das Ändern des Eigentümers einer Domäne jedoch autorisiert werden. Weitere Informationen finden Sie im entsprechenden Thema.

Themen

Wer ist der Eigentümer einer Domäne?

Wenn der Kontakttyp Person ist und Sie die Felder First Name oder Last Name für den Registrierenden ändern, ändern Sie damit den Eigentümer der Domäne.

Wenn der Kontakttyp ein andere Wert als Person ist und Sie Organization ändern, ändern Sie damit den Eigentümer der Domäne.

Beachten Sie Folgendes beim Ändern des Domäneneigentümers:

- Bei einigen TLDs wird für die Änderung des Eigentümers eine Gebühr erhoben. 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 Guthaben nicht verwenden, um die Gebühr zu zahlen, falls eine Gebühr anfällt, um den Inhaber einer Domain zu wechseln.

- Für einige TLDs gilt, wenn Sie den Eigentümer einer Domäne ändern, senden wir eine Autorisierungs-E-Mail an die E-Mail-Adresse des Registrierenden. Der Registrierende muss Sie die Anweisungen in der E-Mail befolgen, um die Änderung zu autorisieren.
- Bei einigen TLDs müssen Sie ein Formular zum Ändern des Domaineigentümers ausfüllen und einen Nachweis der Identität vorlegen, damit ein Amazon-Route-53-Support-Techniker 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 zur Änderung des Besitzers eine spezielle Verarbeitung erfordern

Wenn Sie den Eigentümer einer Domäne ändern, erfordern die Registrierungen für einige TLDs eine spezielle Verarbeitung. 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.

Die folgenden TLDs erfordern zur Änderung des Besitzers der Domäne eine spezielle Verarbeitung:

.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.

- Sie können den Übertragungscode unter https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer anfordern. Befolgen Sie dabei die Eingabeaufforderungen.
- 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 eingeleitet haben, erhalten Sie einen Transferschlüssel für Halter von der E-Mail-Adresse fi-domain-tech@traficom.fi. 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.

So aktualisieren Sie die Kontaktinformationen für eine Domäne

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 die E-Mail-Adresse für den Registranten-Kontakt ändern möchten, führen Sie die folgenden Schritte aus. Wenn Sie die E-Mail-Adresse für den Registranten-Kontakt nicht ändern möchten, 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. Nur Kunden von AISPL (Indien): Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen Verkäufer in Indien. AWS Um den Besitzer einer Domäne zu ändern, wenn die TLD-Registrierung eine Gebühr für die Änderung des Eigentümers berechnet, führen Sie die folgenden Schritte aus, um die Gebühr für die Verlängerung zu bezahlen.

   a. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.

   b. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.

   c. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

      Nachdem Sie die Rechnung bezahlt haben, ändern wir die entsprechenden Einstellungen für den Registrantenkontakt.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um die Einstellungen für den registrierten Kontakt zu ändern, nachdem eine Rechnung storniert wurde, senden Sie die Anforderung erneut.

Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

9. Wenn Sie den Eigentümer einer Domäne ändern, wie unter Wer ist der Eigentümer einer Domäne? 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: • noreply@registrar.amazon.com • noreply@domainnameverification.net

10. 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 UpdateDomainKontakt.

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 Wer ist der Eigentümer einer Domäne?.
- Informationen zum Bestimmen, ob für Ihre Domäne in ein Formular zur Änderung des Domänenbesitzes erforderlich ist, finden Sie unter TLDs, die zur Änderung des Besitzers eine spezielle Verarbeitung erfordern.

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 verwaltete Richtlinie AmazonRoute53 DomainsFull Access 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

   Übernehmen Sie den Standardwert für Account and Billing Support.

Service

Übernehmen Sie den Standardwert Billing.

Kategorie

Übernehmen Sie den Standardwert Domain name registration issue.

Betreff

Geben Sie Change the owner of a domain an.

Beschreibung

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-Abfrage für die Domäne und für die meisten Top-Level-Domains (TLDs) senden und erhält möglicherweise alle Kontaktinformationen, die Sie bei der Registrierung oder bei der Übertragung der Domäne 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 zu einer anderen Vergabestelle übertragen und der Datenschutz für die Domainkontakte aktiviert ist, wird die E-Mail zur Bestätigung der Übertragung von Adressen von identity-protect.org für TLDs zugestellt, die bei der Amazon-Vergabestelle 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.

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 Datenschutz-Service wendet Spam-Schutzfunktionen (Adressrotation und SPF/DKIM/Spam-Analyse) an und leitet E-Mails, die diese Filter passieren, in den meisten Fällen 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.

  Für geografische TLDs, die keinen Datenschutz erlauben, werden Ihre persönlichen Informationen auf der Seite Whois-Verzeichnissuche auf der Gandi-Website mit "als unkenntlich gemacht" gekennzeichnet sind. 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.

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

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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**
   >
   > Falls für Ihre TLD kein Datenschutz unterstützt wird, wird der Abschnitt Datenschutz nicht angezeigt.

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.

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 AWS Guthaben nicht 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 Verlängerungsbenachrichtigungen 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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

Über die Domänenregistrierungen für alle generischen TLDs und viele geografische TLDs können Sie eine Domäne sperren, um zu verhindern, dass die Domäne ohne Ihre Zustimmung an eine andere Vergabestelle übertragen wird. 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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`. Einige TLDs können zusätzlich folgende Statuswerte haben:

- `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. Der automatische Verlängerungszeitraum beträgt in der Regel ein Jahr, wobei einige Top-Level-Domains (TLDs) längere Verlängerungszeiträume haben.

Beachten Sie Folgendes:

Maximaler Verlängerungszeitraum

Alle allgemeinen TLDs und viele Ländercode-TLDs ermöglichen das Verlängern der Domänenregistrierung für längere Zeiträume, in der Regel bis zu zehn Jahren in Ein-Jahres-Schritten. 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.

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. Nur Kunden von AISPL (Indien): Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen Verkäufer in Indien. AWS Um die Registrierung für eine Domäne zu verlängern, führen Sie die folgenden Schritte aus, um die Gebühr für die Verlängerung zu bezahlen.

a. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.

b. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.

c. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

   Nachdem Sie die Rechnung bezahlt haben, schließen wir die Verlängerung ab und senden Ihnen die entsprechenden E-Mails.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um die Domänenregistrierung zu verlängern, nachdem eine Rechnung storniert wurde, übermitteln Sie die Anforderung erneut.

Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

8. 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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-Registrierungsstellen unterstützen häufig Nameserver, die von öffentlichen DNS-Services bereitgestellt wurden, jedoch keine privaten DNS-Server, wie z. B. DNS-Server, die Sie auf Amazon-EC2-Instances konfiguriert haben, es sei denn, die Registrierungsstelle hat IP-Adressen für diese Nameserver. unterstützt nicht die Verwendung von Namenservern, die nicht von der TLD-Registrierungsstelle erkannt werden. 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

Wenn Sie Nameserver für eine .it-Domäne ändern, führt die Registry für eine .it-Domäne eine Überprüfung durch, um sicherzustellen, dass die Nameserver gültig sind. Wenn Sie die falschen Nameserver angeben und die Prüfung fehlschlägt, führt die Registry weitere 22 Tage lang Überprüfungen durch. Während dieser Zeit können Sie die Namen der Namensserver nicht aktualisieren, um den Fehler zu korrigieren, da der EPP-Statuscode `pendingUpdate` ist. 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 AWS dazu, wie Sie Hilfe bei 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 die 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.
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, wobei 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.

Für die meisten Domains oberster Ebene (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 mit Ausnahme von .com.ar, .com.br und .jp verlängern wir die Domainregistrierung 35 Tage vor dem Ablaufdatum, sodass wir Zeit haben, eventuelle Probleme mit der Verlängerung zu lösen, bevor der Domainname abläuft.

Die Registrierungen für die Domains .com.ar, .com.br und .jp erfordern, dass wir die Domains frühestens 30 Tage vor dem Ablaufdatum verlängern. 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.com – Für Domains, deren Vergabestelle Amazon Registrar ist.
- noreply@domainnameverification.net – Für Domains, deren Vergabestelle unsere Partner-Vergabestelle 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**
>
> Einige TLD-Registrierungsstellen lassen ab 25 Tage vor dem Ablaufdatum keine Verlängerung mehr zu, und viele erlauben keine Verlängerung mehr nach dem Ablaufdatum. 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 dem Ende des Zeitraums für späte Verlängerung verlängern oder die Domain versehentlich löschen, erlauben einige Registrierungsdatenbanken für Top-Level-Domains (TLDs) die Wiederherstellung der Domain, bevor sie von Dritten 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 AWS Guthaben nicht 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.

   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 Zeitzone UTC/GMT+1 Stunde gilt. 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

   Übernehmen Sie den Standardwert für Account and Billing Support.

   Service

   Übernehmen Sie den Standardwert Billing.

Kategorie

Übernehmen Sie den Standardwert Domain name registration issue.

Betreff

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

Beschreibung

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 wenn Sie Phone auswählen, 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.

Themen

- Übertragen der Registrierung für eine Domain an Amazon Route 53
- Anzeigen des Status einer Domänenübertragung
- Wie sich das Übertragen einer Domain an Amazon Route 53 auf das Ablaufdatum in der Domainregistrierung auswirkt
- Übertragung einer Domain auf ein anderes AWS Konto
- Überträgt eine Domain von Amazon Route 53 zu einer anderen Vergabestelle.

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 Eigentümerkontaktdaten 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.

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

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

Beachten Sie Folgendes:

AWS Support kontaktieren

Wenn Sie beim Transfer 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.

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 ab, z. B. .com oder .org. 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:

- Kunde TransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod
- Server TransferProhibited

- 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. Wir fügen gelegentlich Unterstützung für weitere TLDs zur Liste hinzu, überprüfen Sie also hin und wieder, ob wir Unterstützung für Ihre Domäne 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.

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.

.es-Domänen

Wenn Sie eine .es-Domäne an Route 53 übertragen, müssen Sie keinen Autorisierungscode angeben.

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 Domäne erhalten, ignorieren Sie die Anweisungen in der E-Mail, da sie für Route 53 nicht relevant sind. Befolgen Sie stattdessen die Anweisungen in diesem Thema.

Verlängern Sie Ihre Domänenregistrierung, bevor Sie die Domäne übertragen (ausgewählte geografische TLDs)

Für die meisten TLDs wird die Registrierung, wenn Sie eine Domain übertragen, automatisch um ein Jahr verlängert. Für einige geografische TLDs wird die Registrierung jedoch nicht verlängert, wenn Sie die Domäne übertragen. Wenn Sie eine Domäne, die über eine dieser TLDs verfügt, an Route 53 übertragen, empfehlen wir, vor der Übertragung der Domäne die Domänenregistrierung zu verlängern, vor allem, 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, .es, .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 Domain-Registranten, 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

Bei einigen Domains oberster Ebene (Top-Level-Domains, TLDs) müssen wir weitere Informationen erfassen. Geben Sie für diese TLDs die entsprechenden Werte hinter dem Feld Postal/Zip Code (PLZ) ein.

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. Nur Kunden von AISPL (Indien): Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen Verkäufer in Indien. AWS Um eine Domain bei Route 53 zu registrieren, führen Sie die folgenden Schritte aus, um die Gebühr für die Registrierung Ihrer Domain zu bezahlen.

    a. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.

    b. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.

    c. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

    Nachdem Sie die Rechnung bezahlt haben, schließen wir die Domainregistrierung ab und senden die entsprechenden E-Mails.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um eine Domain zu registrieren, nachdem eine Rechnung storniert wurde, übermitteln Sie die Anforderung erneut.

    Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

12. 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.com – Für TLDs, die von der Amazon-Vergabestelle registriert wurden.
- noreply@domainnameverification.net Für TLDs, die von unserem Registrierungspartner Gandi registriert wurden. 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.

13. 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.
7. 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.

8. 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.

9. Bei einigen TLDs müssen wir weitere Informationen erfassen. Geben Sie für diese TLDs die entsprechenden Werte hinter dem Feld Postal/Zip Code (PLZ) ein.
10. 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.
11. Wählen Sie Absenden aus.
12. 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.
13. 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.
14. Nur Kunden von AISPL (Indien): Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen Verkäufer in Indien. AWS Um eine Domain bei Route 53 zu registrieren, führen Sie die folgenden Schritte aus, um die Gebühr für die Registrierung Ihrer Domain zu bezahlen.

    a. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.

    b. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.

    c. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

       Nachdem Sie die Rechnung bezahlt haben, schließen wir die Domainregistrierung ab und senden die entsprechenden E-Mails.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um eine Domain zu registrieren, nachdem eine Rechnung storniert wurde, übermitteln Sie die Anforderung erneut.

Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

15. 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.com – Für TLDs, die von der Amazon-Vergabestelle registriert wurden.
    - noreply@domainnameverification.net Für TLDs, die von unserem Registrierungspartner Gandi registriert wurden. 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.

16. 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: Nur Kunden von AISPL (Indien): Zahlen der Übertragungsgebühr

Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung mit Amazon Internet Services Pvt. Ltd (AISPL), einem lokalen AWS Verkäufer in Indien. Um eine Domäne zu Route 53 zu übertragen, führen Sie das folgende Verfahren durch, um die Gebühr für die Übertragung Ihrer Domäne zu bezahlen.

So zahlen Sie die Übertragungsgebühr

1. Wechseln Sie zur Seite Orders and Invoices (Bestellungen und Rechnungen) in der AWS Management Console.
2. Suchen Sie im Bereich Payments Due (Fällige Zahlungen) nach der entsprechenden Rechnung.
3. Wählen Sie in der Spalte Actions (Aktionen) die Option Überprüfen und bezahlen aus.

   Nachdem Sie die Rechnung bezahlt haben, schließen wir die Domänenübertragung ab und senden die entsprechenden E-Mails.

> **Important**
>
> Wenn Sie die Rechnung nicht innerhalb von fünf Tagen bezahlen, wird die Rechnung storniert. Um eine Domäne zu übertragen, nachdem eine Rechnung storniert wurde, übermitteln Sie die Anforderung erneut.

Weitere Informationen finden Sie unter Verwaltung von Zahlungen in Indien im AWS Billing - Benutzerhandbuch.

Schritt 7: Klicken 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 Domäne zu autorisieren.

Generische TLDs wie .com, .net und .org

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

Geographische 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 Wer ist der Eigentümer einer Domäne? beschrieben, senden wir eine E-Mail an den Registrierenden für die Domäne.

E-Mail-Adresse für den Registrierenden (nur für bestimmte TLDs)

Wenn Sie bei einigen TLDs die E-Mail-Adresse für den Registrierenden ändern, senden wir eine E-Mail an die alte und die neue E-Mail-Adresse für den Registrierenden. 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
.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.com • noreply@domainnameverification.net

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**
>
> Da es sich um eine einmalige Gebühr handelt, erscheint die Gebühr nicht in Ihren CloudWatch Abrechnungsstatistiken. Weitere Informationen zu CloudWatch Metriken finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Schritt 8: Aktualisieren der Domänenkonfiguration

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.

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:

- Kunde TransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

Nur geografische TLDs – Überprüfen von 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.

Nur geografische TLDs – Senden einer E-Mail an den Registrierenden für die Übertragungsautorisierung (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.

Nur geografische TLDs – Abwarten der Autorisierung vom Registranten-Kontakt (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**
>
> Für die meisten TLDs können Sie den Registrierungszeitraum für eine Domain auf bis zu zehn Jahre verlängern, nachdem Sie diese an Amazon Route 53 übertragen haben. Weitere Informationen finden Sie unter Verlängern des Registrierungszeitraums für eine Domäne.

Generische 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.

Geografische 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	Geografische TLDs und die Auswirkungen der Übertragung einer Domäne 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	.co.nz, .com.au, .com.sg, .jp, .net.au, .net.nz, .org.nz, .sg – Das Ablaufdatum bleibt unverändert. .in – Es wird ein Jahr zum alten Ablaufdatum hinzugefügt.
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.

Kontinent	Geografische TLDs und die Auswirkungen der Übertragung einer Domäne auf das Ablaufdatum
	.be, de. .fr, .it, .nl – Das neue Ablaufdatum liegt ein Jahr nach dem Datum der Übertragung.

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 verwaltete Richtlinie AmazonRoute53 DomainsFull Access zugewiesen.
- Dem Benutzer wird die FullAccess verwaltete Richtlinie AmazonRoute53 zugewiesen.
- Dem Benutzer wird die Richtlinie PowerUserAccess Managed zugewiesen.
- Der Benutzer verfügt über die Berechtigung zum Ausführen aller folgenden Aktionen: `TransferDomainsDisableDomainTransferLock` 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 möchten 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 das AWS CLI, eines der AWS SDKs oder die 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 und Toolkits“ im Abschnitt Anleitungen und API-Referenzen auf der Seite „AWS Dokumentation“.
- Das empfangende Konto hat drei Tage Zeit, um die Übertragung aus dem ursprünglichen Konto unter Verwendung der API transfer-domain-to-another-aws-account zu akzeptieren. Wenn die Übertragung nicht innerhalb von drei Tagen akzeptiert wurde, wird die Übertragungsanforderung abgebrochen.

> **Important**
>
> Wenn Sie eine Domain programmgesteuert 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 Konto AWS.

Schritt 2 (optional): Migrieren Sie eine gehostete Zone auf ein anderes Konto AWS

Wenn Sie Route 53 als DNS-Service für die Domäne verwenden, überträgt Route 53 die gehostete Zone nicht, wenn Sie eine Domäne 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, von dem Sie die Domain übertragen, als auch das Konto, auf das Sie die Domain übertragen, besitzen, 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 gehosteten Zone zu einem anderen AWS Konto.

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.

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 Domäne bei der aktuellen Vergabestelle registriert haben oder die Registrierung für die Domäne der aktuellen Vergabestelle vor mindestens 60 Tagen 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:
  - pendingDelete
  - pendingTransfer

- redemptionPeriod
- Kunde TransferProhibited

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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
- Kunde TransferProhibited
- Server TransferProhibited

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 Server istTransferProhibited, 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.

> **Note**
>
> Wenden Sie sich an den AWS Support, um den Registrar-Transfer von .jp-Domains freizuschalten. Weitere Informationen finden Sie unter Wenden Sie sich AWS bei Problemen mit der Domainregistrierung an den Support.

6. Alle Domains außer den Domains.be-, .co.za-, .es-, .ru-, .uk-, .co.uk-, .me.uk- und .org.uk-Domains — Wählen Sie auf der Domainnamenseite im Drop-down-Menü Transfer out die Option An einen 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.

   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 Belgium.

.co.za-Domänen

Sie benötigen keinen Autorisierungscode, um eine .co.za-Domäne auf eine andere Vergabestelle zu übertragen.

.es-Domänen

Sie benötigen keinen Autorisierungscode, um eine .es-Domäne an eine andere Vergabestelle zu übertragen.

.ru-Domänen

Rufen Sie den Autorisierungscode von der Registrierungsstelle für .ru-Domänen unter https://www.nic.ru/en/auth/recovery/ ab:

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. Klicken Sie auf der Seite Registered Domains (Registrierte Domänen) > auf domain name (Domänenname), dann unter IPS Tag auf Change IPS Tag (IPS-Tag ändern) und geben Sie den Wert aus Schritt 7a an.
c. Wählen Sie Aktualisieren.

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, .es, .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 zu https://approvemove.com enthalten, wo Sie die Übertragung genehmigen oder ablehnen können. Wenn der Datenschutz für die Domainkontakte aktiviert ist, wird die E-Mail von identity-protect.org-Adressen für TLDs zugestellt, die bei der Amazon-Vergabestelle 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 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 der neue Registrar meldet, dass die Übertragung fehlgeschlagen ist, weil der Autorisierungscode, den Sie von Route 53 erhalten haben, nicht gültig ist, wenden Sie sich an den 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.

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 des Registrars an Amazon Registrar

Amazon Route 53 Domains verwendet zwei Registrare, um Domains für Kunden zu registrieren: Amazon Registrar, ein Registrar, der Eigentum ist und von diesem betrieben wird AWS, und Gandi, einen Registrar-Partner, mit dem wir zusammenarbeiten. Anfänglich wurden die meisten Route 53-Domains über Gandi registriert, da Amazon Registrar für viele Top-Level-Domains (TLDs) wie .com oder .club nicht direkt akkreditiert war. Jetzt, da Amazon Registrar direkt mit Hunderten von TLDs akkreditiert ist (und es werden immer mehr), werden wir in Ihrem Namen damit beginnen, über Gandi registrierte Domains an Amazon Registrar zu übertragen.

Dadurch wird nichts daran geändert, wie Sie die Domain innerhalb von Route 53 verwalten. Es wird lediglich der Registrar of Record für Ihre Domain von Gandi auf Amazon Registrar aktualisiert. Die Übertragung erfolgt während des Domainverlängerungsprozesses und es fallen nur die üblichen Verlängerungsgebühren an. Nach Abschluss der Übertragung können sich neue Anfragen zur Übertragung Ihrer Domain an einen anderen Registrar AWS verzögern. Route 53 informiert die betroffenen Domain-Registranten 15 Tage vor der Übertragung über die Verlängerung. Dieser

Vorgang ist in unserer Vereinbarung zur Registrierung von Domainnamen beschrieben (siehe Abschnitt 3.11.5).

Diese Übertragung ist erforderlich, wenn Sie den Route 53-Service weiterhin zur Verwaltung Ihrer Domains nutzen möchten. Wenn Sie Amazon Registrar nicht für die Verwaltung Ihrer Domain verwenden möchten, müssen Sie Ihre Domain innerhalb von 15 Tagen nach Erhalt der Übertragungsmitteilung bei der Verlängerung von zu einem anderen Registrar übertragen. AWS

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:

Registrieren einer Domäne

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.

Nur geografische TLDs – Übertragen einer Domain an Amazon Route 53

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.

Domäne löschen

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.

Nur geografische TLDs – Übertragen einer Domain von Route 53 zu einer anderen Vergabestelle

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
- Erneutes Senden von E-Mails

Aktualisieren Ihrer E-Mail-Adresse

Wir senden immer Bestätigungs-E-Mails und Autorisierungs-E-Mails an die Adresse des Registrierenden für eine Domäne. Bei einigen TLDs müssen wir in folgenden Fällen eine E-Mail an die alte und die neue E-Mail-Adresse des Registrierenden 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
.fr	nic@nic.fr
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Die E-Mail enthält einen Link zu https://approve.domainadmin.com.
.fr	nic@nic.fr
Alle anderen	Eine der folgenden E-Mail-Adressen: • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.com • noreply@domainnameverification.net

> **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 hierfür zwei Möglichkeiten:
   - 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.
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-Datenverkehrs, 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

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 GetDomainDetail-API anzuzeigen, können Sie eines der SDKs oder AWS CLI verwenden. 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

Sie können Informationen zu Domains anzeigen, die unter Verwendung von Route 53 registriert wurden. Zu diesen Informationen gehören Informationen wie das Datum, an dem die Domain ursprünglich registriert wurde, und Kontaktinformationen für den Domaininhaber sowie für die technischen, administrativen und Rechnungskontakte.

WHOIS

WHOIS ist ein kostenloses, öffentlich zugängliches Verzeichnis mit Informationen zu Domains, die von Domainvergabestellen und Registrierungsstellen gesponsert werden. Es wird sowohl als Service, der Abfragen am Port 43 akzeptiert, als auch als Website bereitgestellt. Auf beides kann sowohl über IPv4 als auch über IPv6 zugegriffen werden. 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 Richtlinien für die zulässige Nutzung, einschließlich unangemessener Inhalte, Phishing, Malware oder Spam, zu melden, senden Sie eine E-Mail an abuse@amazon.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: https://registrar.amazon.com/whois

- Amazon Registrar RDAP: https://registrar.amazon.com/rdap
- 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

Für die meisten Domains oberster Ebene (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, mit denen Sie eine Domainregistrierung löschen können

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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.com – Für TLDs, die von der Amazon-Vergabestelle registriert wurden.
   - noreply@domainnameverification.net – Für TLDs, die von unserem Registrierungspartner Gandi registriert wurden.

   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 die Löschanfrage 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 (stornieren), wird er am Ende des Tages gelöscht und steht jedem zur Registrierung zur Verfügung. 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
- AWS Support kontaktieren, wenn Sie sich nicht bei Ihrem AWS Konto anmelden können

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 Center 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. Geben Sie die folgenden Werte an:

   Regarding

   Übernehmen Sie den Standardwert für Account and Billing Support.

   Service

   Akzeptieren Sie den Standardwert Domains.

   Kategorie

   Akzeptieren Sie den Standardwert für Registration Issue.

   Schweregrad

   Wählen Sie den zutreffenden Schweregrad.

   Betreff

   Geben Sie eine kurze Zusammenfassung des Problems ein.

   Beschreibung

   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.

3. 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 Ihre AWS Rechnung von einer Kreditkarte abgebucht wird, erhalten Sie für jede Domain-Transaktion eine separate Rechnung. Diese Rechnungen enthalten den Domainnamen nicht. 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
- Ändern des Eigentümers einer Domain (für einige TLDs ist dieser Vorgang kostenlos)

> **Note**
>
> Wenn Sie Zahlungen auf Rechnung verwenden, erscheinen alle Route-53-Domainregistrierungstransaktionen auf Ihrer monatlichen AWS Rechnung. Die Rechnung enthält den Domainnamen und den Vorgang, für den jede Gebühr gilt.

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 Rechnungsbericht im CSV-Format enthält die folgenden Werte:

- Die AWS Rechnungs-ID, auf der die Gebühr erscheint.
- Der Vorgang (REGISTER_DOMAIN, RENEW_DOMAIN, TRANSFER_IN_DOMAIN oder CHANGE_DOMAIN_OWNER).
- Der Name der Domain.
- Die Gebühr für den Vorgang in US-Dollar.
- Das Datum und die Uhrzeit im ISO 8601-Format, z. B. 2016-03-03T19:20:25.177Z. Weitere Informationen über das ISO 8601-Format finden Sie im Wikipedia-Artikel ISO 8601.

So laden Sie einen Domains-Rechnungsbericht herunter

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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**
>
> Der Route 53-DNS-Dienst kann mit jeder Top-Level-Domain Ihrer Wahl und mit jedem Domain-Registrar verwendet werden. Die Informationen auf dieser Seite beziehen sich nur auf die Domänen, die Sie bei Route 53 registrieren können. Weitere Informationen zu Route 53 als DNS-Dienst finden Sie unter. Wie Internetdatenverkehr an Ihre Website oder die Webanwendung geleitet wird

Die nachfolgend aufgelisteten generischen und geografischen Top-Level-Domains zeigen die Domains der obersten Ebene (TLDs), die Sie verwenden können, um Domains mit Amazon Route 53 zu registrieren.

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. Die 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.

Im Fall der meisten TLDs müssen Sie einen Autorisierungscode aus der aktuellen Vergabestelle abrufen, um eine Domain zu übertragen. Informationen dazu, ob Sie einen Autorisierungscode benötigen, finden Sie im Abschnitt „Autorisierungscode erforderlich für die Übertragung zu Route 53" “ 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 Auflistung für jede TLD gibt an, ob diese TLD IDNs unterstützt. Weitere Informationen zu internationalisierten Domainnamen finden Sie unter Format für DNS-Domänennamen.

Registrieren von geografischen Domains bei TLDs

Die Regeln für die Registrierung von geografischen TLDs unterscheiden sich 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, .bieten, .bike, .bingo, .bio, .biz, .black, .blue, .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, .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, . Ventilator, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, . 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, .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, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

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, . einkaufen, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, . Software, .space, .store, .streamen, .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, . arbeiten, .works, .world, .wtf, .xyz, .zone

Geografische Top-Level-Domains

Afrika

.ac (Ascension), .co.za (Südafrika), .sh (St. Helena)

Nord- und Südamerika

.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), .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 erkannt 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, .bieten, .bike, .bingo, .bio, .biz, .black, .blue, .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, .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, . Ventilator, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, . 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, .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, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

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, . einkaufen, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, . Software, .space, .store, .streamen, .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, . arbeiten, .works, .world, .wtf, .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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.bieten

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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 zu CEOs und deren Gleichgestellten 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. 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 Registrierung 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

. Ventilator

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

.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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

.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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Verisign, die Registrierungsstelle für .name-TLDs, ermöglicht das Registrieren von Domains zweiter Ebene (Name.name) und dritter Ebene (Vorname.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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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 Arabisch, Weißrussisch, Bosnisch, Bulgarisch, Chinesisch (vereinfacht und traditionell), Dänisch, Deutsch, Hindi, Ungarisch, Isländisch, Koreanisch, Litauisch, Lettisch, Mazedonisch, Polnisch, Russisch, Serbisch und Spanisch.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

.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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

.streamen

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum

- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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, Webfernsehen, Videos oder Armbanduhren 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach Ablauf
- Wiederherstellung mit der Registrierung möglich: Zwischen 45 Tagen und 75 Tagen nach Ablauf
- Domain wird aus der Registrierung gelöscht: 75 Tage nach Ablauf

. arbeiten

Return to index

Lease-Zeitraum für Registrierung und Verlängerung

Ein bis zehn Jahre.

Datenschutz (gilt für alle Kontaktarten: Personen, Unternehmen, Vereinigungen und öffentliche Einrichtungen)

Alle Informationen sind verborgen, außer dem Organisationsnamen.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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 Domainerweiterungen werden nach geografischer Lage gruppiert und enthalten offizielle länderspezifische Erweiterungen, bekannt als Ländercode-Domains oberster Ebene (ccTLDs). Zu den Beispielen gehören .be (Belgien), .in (Indien) und .mx (Mexiko). Die Regeln für die Registrierung von ccTLDs sind regional unterschiedlich. 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 aller ccTLDs auf Route 53, mit Ausnahme von .cc und .tv, werden Aktualisierungen des Eigentümerkontakts ignoriert und die Eigentümerkontaktdaten 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

.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), .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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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

Nicht unterstützt Um unbefugte Übertragungen zu verhindern, schränken Sie den Zugriff auf die E-Mail-Adresse des Registranten und auf die Route 53-APIs ein, die einen Eigentümerwechsel ermöglichen könnten, z. B. Kontakt. UpdateDomain Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domains in der Service-Autorisierungs-Referenz und Beispielberechtigungen für einen Domänendatensatzbesitzer.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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 Nord- und Südamerika verwenden, um Domains bei Amazon Route 53 zu registrieren.

, , , , , , , , ,

Return to index

.ca (Kanada)

Return to index

Varianten eines Domainnamens mit (à) oder ohne (a) eines Akzentzeichens 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: Ihre/Seine Majestät der/die König(in)
- 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf

- Domain wird aus Route 53: 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

Die Registrierungsstelle für .co-Domains (Go.co) betrachtet einige Domainnamen als Premium-Domainnamen. Sie können keine Premium-.co-Domains in Route 53 registrieren oder dorthin übertragen. Weitere Informationen finden Sie auf der Go.co- Website.

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 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, beschränken Sie den Zugriff auf die E-Mail-Adresse des Registranten und auf die Route 53-APIs, die einen Eigentümerwechsel ermöglichen könnten, z. B. Kontakt. UpdateDomain Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domains in der Service-Autorisierungs-Referenz und Beispielberechtigungen für einen Domänendatensatzbesitzer.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 Jahr.

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.
- 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.
- Die ID-Nummer, die eine Medicare-Krankenversicherungsnummer, eine Steuerdateinummer (TFN), eine staatliche Führerscheinnummer oder eine australische Geschäftsnummer (ABN) sein kann.
- Ihr Bundesstaat oder Provinz.

- 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 .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

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 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

Sie können die folgenden Domains zweiter Ebene mit Route 53 registrieren: .co.nz, .net.nz und .org.nz. Sie können keine .nz-Domains (oberste Ebene) mit Route 53 registrieren oder .nz-Domains an Route 53 übertragen.

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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von 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 Bundesstaat oder Provinz.
- 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 Um unbefugte Übertragungen zu verhindern, schränken Sie den Zugriff auf die E-Mail-Adresse des Registranten und auf die Route 53-APIs ein, die einen Eigentümerwechsel ermöglichen könnten, z. B. Kontakt. UpdateDomain Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domains in der Service-Autorisierungs-Referenz und Beispielberechtigungen für einen Domänendatensatzbesitzer.

Internationalisierte Domainnamen

Unterstützt für Japanisch.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja.

Autorisierungscode erforderlich für die Übertragung von Route 53

Ja.

DNSSEC

Nicht unterstützt

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Zwischen 30 und 7 Tagen 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 sind ausgeblendet, mit Ausnahme von Bundesstaat/Provinz und Land.

Domainsperre zum Verhindern unautorisierter Übertragungen

Unterstützt.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 Registry 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

Nur Domains zweiter Ebene sind verfügbar. Route 53 unterstützt die Domains zweiter Ebene .com.au und net.au.

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 Bundesstaat oder Provinz.
- 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

Sie können die folgenden Domains zweiter Ebene mit Route 53 registrieren: .co.nz, .net.nz und .org.nz. Sie können keine .nz-Domains (oberste Ebene) mit Route 53 registrieren oder .nz-Domains an Route 53 übertragen.

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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von 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

Sie können die folgenden Domains zweiter Ebene mit Route 53 registrieren: .co.nz, .net.nz und .org.nz. Sie können keine .nz-Domains (oberste Ebene) mit Route 53 registrieren oder .nz-Domains an Route 53 übertragen.

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, dass Sie unbefugte Übertragungen 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von 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, einem Inselstaat in der Mikronesien-Subregion Ozeaniens im westlichen Pazifik, vorbehalten. 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: gelöscht: 45 Tage nach 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 API-Aktion einschränken. RetrieveDomainAuthCode (Wenn Sie den Zugriff auf diese Route 53-API einschränken, schränken Sie auch ein, wer mithilfe der Route 53-Konsole, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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, dass Sie unbefugte Übertragungen 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja. Den Transfercode finden Sie auf der Website von DNS Belgium.

Autorisierungscode erforderlich für die Übertragung von Route 53

Ja. Den Transfercode erhalten Sie auf der Website von DNS Belgium.

DNSSEC

Für die Domainregistrierung unterstützt. Weitere 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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. Weitere Informationen zum Verifizieren von Namensservern für Ihre Domain finden Sie unter https://www.denic.de/en/service/tools/nast/.

Datenschutz

Nicht unterstützt

Domainsperre zum Verhindern unautorisierter Übertragungen

Nicht unterstützt Wir empfehlen, dass Sie unbefugte Übertragungen 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren

kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere 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 neue .es-Domains gekauft oder in Route 53 übertragen werden, wenn der Kontakttyp für den Registrierenden eine Person ist. Sie können .es-Domains nicht kaufen oder übertragen, wenn der Kontakttyp für den Registrierenden ein Unternehmen, eine Vereinigung oder eine öffentliche Einrichtung ist.
> Der Kontakttyp für den Registranten-Kontakt kann auch nicht in Firma geändert werden.

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-ID ähnlich wie *AAAA0-ESNIC-F0*.
- 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 auf https://www.nic.es/sgnd/login.action an, indem Sie Ihre ESNIC-ID 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.action?request_locale=en.

  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

Nicht unterstützt Um unbefugte Übertragungen zu verhindern, beschränken Sie den Zugriff auf die E-Mail-Adresse des Registranten und auf die Route 53-APIs, die einen Eigentümerwechsel ermöglichen könnten, z. B. Kontakt. UpdateDomain Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Route 53-Domains in der Service-Autorisierungs-Referenz und Beispielberechtigungen für einen Domänendatensatzbesitzer.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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 sein und ihr Geburtsdatum angeben.
- 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.
- Wenn Sie Unternehmen, Vereinigung oder öffentliche Einrichtung als Kontakttyp eingeben, ist eine USt-ID (Umsatzsteuernummer) erforderlich.
- 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, dass Sie unbefugte Übertragungen 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt.

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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, dass Sie unbefugte Übertragungen 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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Nicht unterstützt

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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).

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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.

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, AWS SDKs und anderen programmgesteuerten Methoden einen Autorisierungscode generieren kann.) Weitere Informationen finden Sie unter Identity and Access Management in Amazon Route 53.

Internationalisierte Domainnamen

Unterstützt für Latein, Schwedisch und Jiddisch.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die 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

Autorisierungscode erforderlich für die Übertragung zu Route 53

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.

Autorisierungscode erforderlich für die Übertragung zu Route 53

Ja

DNSSEC

Für die Domainregistrierung unterstützt. Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Domäne.

Fristen für die Verlängerung und Wiederherstellung von Domains

- Verlängerung möglich: Bis zum Ablaufdatum
- Späte Verlängerung mit Route 53 möglich: Bis zu 44 Tage nach Ablauf
- Domain wird aus Route 53: 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.

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

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 mit einem Experten Kontakt unter AWS aufnehmen möchten, 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 7: Aktualisieren Sie die NS-Einträge, um Route 53-Nameserver zu verwenden
- Schritt 8: Überwachen des Datenverkehrs für die Domäne
- Schritt 9: Zurückändern der TTL für den NS-Datensatz in einen höheren Wert
- Schritt 10: Übertragen der Domänenregistrierung an Amazon Route 53
- Schritt 11: DNSSEC-Signatur erneut aktivieren (falls erforderlich)

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 Domänennamen in einen Webbrowser eingibt, soll der Datenverkehr an den Webserver in Ihrem Rechenzentrum, auf eine Amazon-EC2-Instance, an eine CloudFront-Verteilung oder an einen anderen Ort geleitet werden?

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-Datensätzen erläutert die Vorteile von Route 53-Aliasdatensätzen, die den Datenverkehr für bestimmte AWS-Ressourcen wie CloudFront-Verteilungen und Amazon S3-Buckets kostenlos 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-Datensätze (Adresse) - Einem Domänen- oder Subdomänennamen die IPv4-Adresse (z. B. 192.0.2.3) der entsprechenden Ressource zuordnen
- AAAA-Datensätze (Adresse) - Einem Domänen- oder Subdomänennamen die IPv6-Adresse (z. B. 2001:0db8:85a3:0000:0000:abcd:0001:2345) der entsprechenden Ressource zuordnen
- 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 der AWS Management Console an und öffnen Sie die Route 53 -Konsole unter https://console.aws.amazon.com/route53/.
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 Domänennamen 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 den Datenverkehr für example.com und www.example.com an einen Webserver auf einer Amazon EC2 Instance weiterleiten möchten, erstellen Sie zwei Datensätze, und zwar 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 EC2-Instance an.

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 eines der AWS SDKs, die AWS CLI oder AWS Tools for Windows PowerShell verwenden. Weitere Informationen finden Sie in der AWSDokumentation.

Wenn Sie eine Programmiersprache verwenden, für die AWS kein SDK zur Verfügung stellt, können Sie auch die Route 53 API nutzen. 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 AWS Management Console an 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, DNSSEC-Signatur für zwei Anbieter aktiviert zu haben, müssen Sie alle DS oder DNSKEYs entfernen, um DNSSEC zu 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 AWS Management Console an 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 AWS Management Console an 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 an, dass Route 53 einen Key Signing Key (KSK) basierend auf einem vom Kunden verwalteten Schlüssel in AWS Key Management Service (AWS KMS) enthalten.
- 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 Domänennamen in einen Webbrowser eingibt, soll der Datenverkehr an den Webserver in Ihrem Rechenzentrum, auf eine Amazon-EC2-Instance, an eine CloudFront-Verteilung oder an einen anderen Ort geleitet werden?

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-Datensätzen erläutert die Vorteile von Route 53-Aliasdatensätzen, die den Datenverkehr für bestimmte AWS-Ressourcen wie CloudFront-Verteilungen und Amazon S3-Buckets kostenlos 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-Datensätze (Adresse) - Einem Domänen- oder Subdomänennamen die IPv4-Adresse (z. B. 192.0.2.3) der entsprechenden Ressource zuordnen
- AAAA-Datensätze (Adresse) - Einem Domänen- oder Subdomänennamen die IPv6-Adresse (z. B. 2001:0db8:85a3:0000:0000:abcd:0001:2345) der entsprechenden Ressource zuordnen
- 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 der AWS Management Console an 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 (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 Domänennamen 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 den Datenverkehr für example.com und www.example.com an einen Webserver auf einer Amazon EC2 Instance weiterleiten möchten, erstellen Sie zwei Datensätze, und zwar 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 EC2-Instance an.

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 eines der AWS SDKs, die AWS CLI oder AWS Tools for Windows PowerShell verwenden. Weitere Informationen finden Sie in der AWSDokumentation.

Wenn Sie eine Programmiersprache verwenden, für die AWS kein SDK zur Verfügung stellt, können Sie auch die Route 53 API nutzen. 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

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.

Um anzugeben, wie Route 53 den Datenverkehr für die Domäne weiterleiten soll, erstellen Sie Datensätze in der gehosteten Zone. Wenn Sie beispielsweise möchten, dass Anfragen an example.com an einen Webserver weitergeleitet werden, der auf einer Amazon-EC2-Instance ausgeführt wird, erstellen Sie einen Datensatz in der gehosteten Zone example.com und geben Sie 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 den Verkehr zu ausgewählten AWS Ressourcen weiterleiten, finden Sie unterWeiterleitung 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.

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 öffentliche gehostete Zone, wenn Sie möchten, dass Internetdatenverkehr zu Ihren Ressourcen geleitet wird, sodass Ihre Kunden beispielsweise die Unternehmens-Website anzeigen 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-Datensatz in der gehosteten Zone für die Domäne (example.com) und geben die vier Namensserver an, die Sie in Schritt 3 erhalten haben.

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.

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**
>
> Während wir hier den Prozess zum Erstellen und Delegieren an eine Subdomänen-gehostete Zone auf Route 53 beschreiben, können Sie auch eine DNS-Zone auf anderen Nameservern erstellen und in ähnlicher Weise Namenserver-Einträge (NS) erstellen, die die Verantwortung an diese Nameserver delegieren.

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 AWS Management Console an 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 Domänennamen 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 Subdomäne ein.

   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 gehosteten 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 Datenverkehr für www.example.com zu einer CloudFront-Verteilung oder einem 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 für die Weiterleitung des Datenverkehrs innerhalb mindestens einer der von Ihnen mit dem Amazon VPC-Service erstellten VPC verwenden. 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 unter CreateCloudFrontOriginAccessIdentity in 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.

> **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.

So erstellen Sie eine öffentlich gehostete Zone mit der Route 53-Konsole

1. Melden Sie sich bei der AWS Management Console an 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 (Erstellte gehostete Zone).
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 Domänennamen 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 AWS Management Console an 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.

Auflisten der öffentlichen gehosteten Zonen

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. Weitere Informationen zum Auflisten von gehosteten Zonen mithilfe der Route 53-API finden Sie unter ListHostedZones im Amazon Route 53 — API-Referenz.

So listen Sie mithilfe der Route 53-Konsole die mit einem AWS-Konto verknüpfen öffentlichen gehosteten Zonen auf

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Route 53-Konsole unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen). Die Seite zeigt Hosted Zones (Gehostete Zonen) an, die mit dem AWS-Konto verknüpft sind, über das 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 CloudWatch angezeigt. Hier können Sie ein Diagramm anzeigen, den Zeitraum auswählen, den Sie anzeigen möchten, und die Metriken auf verschiedene andere Weise anpassen. 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 für alle öffentlichen gehosteten Zonen an CloudWatch, sodass Sie keine Einstellungen konfigurieren müssen, bevor Sie 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 mithilfe der AWS CLI, müssen Sie entweder die AWS-Region nicht angegeben, oder geben `us-east-1` als Region ein. Route 53 Metriken sind nicht verfügbar, wenn Sie eine andere Region auswählen.

CloudWatch-Metrik und -Dimension für DNS-Abfragen

Weitere Informationen zur CloudWatch-Metrik und -Dimension für DNS-Abfragen finden Sie unter Überwachung von Hosting-Zonen mit Amazon CloudWatch. Weitere Informationen zu CloudWatch Metriken und Alarme finden Sie unter Amazon-CloudWatch-Konzepte im Amazon-CloudWatch-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:

- Die angeforderte Domain oder Subdomain
- Das Datum und die Uhrzeit der Anforderung
- DNS-Datensatztyp (z. B. A oder AAAA)
- Der Route 53-Edge-Standort, 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 einmal pro Minute Metriken und Dimensionen an CloudWatch zu senden. Sie können mithilfe der folgenden Verfahren die Metriken in der CloudWatch-Konsole oder mithilfe von AWS Command Line Interface (AWS CLI) anzeigen.

Themen

- Anzeigen von DNS-Abfragemetriken für eine öffentliche gehostete Zone in der CloudWatch-Konsole
- Abrufen von DNS-Abfragemetriken mithilfe der AWS CLI

Anzeigen von DNS-Abfragemetriken für eine öffentliche gehostete Zone in der CloudWatch-Konsole

Um DNS-Abfragemetriken für öffentliche gehostete Zonen in der CloudWatch-Konsole anzuzeigen, führen Sie die folgenden Schritte aus.

So zeigen Sie DNS-Abfragemetriken für eine öffentliche gehostete Zone in der CloudWatch-Konsole an

1. Melden Sie sich bei AWS Management Console an 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 oberen rechten Ecke des Konsolenfensters US East (N. Virginia) (USA Ost (Nord-Virginia)) über die AWS Regionsauswahl aus. Route 53-Metriken sind nicht verfügbar, wenn Sie andereAWSRegion :
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 gehostete Zonen mit dem Metriknamen DNSQueries.
7. Ändern Sie auf der Registerkarte Graphed metrics (Grafische Metriken) die entsprechenden Werte, um die Metriken im gewünschten Format anzuzeigen.

   Wählen Sie für Statistic (Statistik) die Option Sum (Summe) oder SampleCount aus. Diese Statistiken zeigen beide denselben Wert an.

Abrufen von DNS-Abfragemetriken mithilfe der AWS CLI

Um DNS-Abfragemetriken mithilfe der AWS CLI abzurufen, verwenden Sie den Befehl get-metric-data. 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.
- Belassen Sie entweder dieAWSRegion nicht angegeben, oder geben Sie`us-east-1`als Region. Route 53 Metriken sind nicht verfügbar, wenn Sie eine andere Region auswählen. Weitere Informationen finden Sie unter Konfigurieren der AWS CLI im AWS Command Line Interface Benutzerhandbuch.

Hier ist der AWS CLI-Befehl, den Sie verwenden, um DNS-Abfragemetriken für den Fünf-Minuten-Zeitraum zwischen 4:01 und 4:07 am 1. Mai 2019 abzurufen. 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
- Löschen von öffentlichen gehosteten Zonen, die von einem anderen Dienst erstellt wurden
- Löschen einer öffentlichen gehosteten Zone mit der Route 53-Konsole.

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 AWS Cloud Map erstellt hat, als Sie einen öffentlichen DNS-Namespace erstellt haben, löschen Sie den Namespace. AWS Cloud Map löscht die gehostete Zone automatisch. Weitere Informationen finden Sie unter Löschen von Namespaces im AWS Cloud MapEntwicklerleitfaden.
- 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 AWS Management Console an 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:

   - 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 Delete (Löschen).
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 Geolokations-, Geoproximitäts- und Latenzdatensätze können Sie auch Abfragen von einem bestimmten DNS-Resolver und/oder einer bestimmten Client-IP-Adresse simulieren, um zu ermitteln, 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 AWS Management Console an 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.
   - Für Alias-Datensätze, die sich auf AWS-Ressourcen und nicht auf einen weiteren Datensatz beziehen, enthält die Antwort eine IP-Adresse oder einen Domänennamen für die AWS-Ressource und je nach Typ der 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 AWS Management Console an 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- oder IPv6-Adresse an, um den Standort des DNS-Resolvers anzugeben, den ein Client für Anforderungen verwendet. Dies ist für das Testen von Datensätzen für Latenz und Geolokation hilfreich. Wenn Sie diesen Wert nicht angeben, verwendet das Werkzeug die IP-Adresse eines DNS-Resolvers in der AWS-Region USA Ost (Nord-Virginia) (us-east-1).

   EDNS0 client subnet 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 IPv6-Adressen.

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.
- Für Alias-Datensätze, die sich auf AWS-Ressourcen und nicht auf einen weiteren Datensatz beziehen, enthält die Antwort eine IP-Adresse oder einen Domänennamen für die AWS-Ressource und je nach Typ der 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

White-Label-Name-Server sind einem wiederverwendbaren Route 53-Delegierungssatz zugeordnet. Sie können White-Label-Name-Server nur dann für eine gehostete Zone verwenden, wenn die

gehostete Zone und der wiederverwendbare Delegierungssatz von demselben AWS-Konto erstellt wurden.

Um eine wiederverwendbare Delegierungsgruppe zu erstellen, können Sie die Route 53-API, AWS-CLI oder die AWS SDKs verwenden. Weitere Informationen finden Sie in der folgenden Dokumentation:

- Route 53 — API— Siehe CreateReusableDelegationSet im Amazon Route 53 — API-Referenz
- AWS-CLI Siehe create-reusable-delegation-setAWS CLI im
- AWS SDKs – Siehe die jeweilige SDK-Dokumentation auf der Seite für die AWS-Dokumentation

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 unterCreateHostedZone in 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 gehosteten Zonen und Festlegen einer wiederverwendbaren Delegierungsgruppe für die Nameserver für die gehosteten Zonen finden Sie unter CreateHostedZone in Amazon Route 53 API Reference.

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.

  Weitere Informationen zum Erstellen von Verteilungen über die Route 53-API finden Sie unter CreateDistribution in 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 die IPv4- und IPv6-Adressen der Nameserver in der wiederverwendbaren Delegierungsgruppe 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 Ihrer wiederverwendbaren Delegierungsgruppe.

> **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. Fügen Sie sowohl die IPv4- als auch die IPv6-Adresse für einen White-Label-Nameserver in den entsprechenden Glue-Datensatz ein, z. B.:

     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: Ändern der TTLs auf die ursprünglichen Werte

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-Dienstes, welche die edns-client-subnet-Erweiterung von EDNS0 unterstützen, und teilen Sie ihnen die Namen Ihrer White-Label-Nameserver mit. 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 AWS Management Console an 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 das Erhöhen dieser TTLs, die für negative Antworten für die gesamte gehostete Zone gelten, 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 AWS Management Console an 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.

Arbeiten mit privat gehosteten Zonen

Eine privat gehostete Zone ist ein Container mit Informationen darüber, wie Amazon Route 53 auf DNS-Abfragen für eine Domäne und deren Subdomänen innerhalb mindestens einer von Ihnen mit dem Amazon VPC-Service erstellten VPC reagieren soll. 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. In der gehosteten Zone erstellen Sie Datensätze, die bestimmen, wie Route 53 DNS-Abfragen für Ihre Domäne und Subdomänen innerhalb und zwischen Ihren VPCs beantworten soll. Nehmen wir beispielsweise an, Sie haben einen Datenbankserver, der auf einer EC2-Instance in der VPC ausgeführt wird, die Sie der privat gehosteten 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 privat gehosteten Zone zu erhalten, müssen Sie außerdem eine EC2-Instance in einer der zugehörigen VPCs ausführen (oder über

einen eingehenden Endpunkt aus einem Hybrid-Setup verfügen). Wenn Sie versuchen, eine private gehostete Zone von außerhalb der VPCs oder Ihres Hybrid-Setups abzufragen, wird die Abfrage im Internet rekursiv 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 Route 53 Resolver in einer VPC abfragen, die der gehosteten Zone zugeordnet wurde, indem Sie einen eingehenden Endpunkt verwenden, der mit den in der privaten gehosteten Zone angegebenen VPCs verbunden ist.

Während die Nameserver im Internet sichtbar sind, stellt Route 53 Resolver keine Verbindung zu den Nameserver-Adressen her. Außerdem werden die Informationen zur privaten gehosteten Zone nicht zurückgegeben, wenn Sie die Nameserver direkt über das Internet abfragen. Stattdessen erkennt der Route 53 Resolver, dass sich Abfragen in einem privaten Namespace befinden, der auf Zuordnungen von VPCs 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 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 Anzeigen und Aktualisieren der DNS-Unterstützung für Ihre VPC im Amazon-VPC-Benutzerhandbuch.

Route 53 Zustandsprüfungen

In einer privaten gehosteten Zone können Sie Route-53-Zustandsprüfungen nur mit Failover und mehrwertigen Antworten sowie mit gewichteten, Latenz- und Geolokalisierungsdatensätzen 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
- Routing mit Geoproximität

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. Verknüpfen Sie eine oder mehrere Amazon VPCs mit der privaten gehosteten Zone. Route 53 Resolver verwendet die private gehostete Zone, um DNS-Abfragen in den angegebenen VPCs weiterzuleiten.
3. Erstellen Sie Datensätze in jeder gehosteten Zone. Datensätze in der öffentlichen gehosteten Zone steuern, wie Internetdatenverkehr weitergeleitet wird, und Datensätze in der privaten gehosteten Zone steuern, wie der Datenverkehr in Ihren Amazon VPCs weitergeleitet wird.

Wenn Sie die Namensauflösung Ihrer VPC und Ihrer On-Premises-Workloads durchführen müssen, können Sie Route 53 Resolver verwenden. Weitere Informationen finden Sie unter Was ist? Amazon Route 53 Resolver.

Öffentliche und private gehostete Zonen mit überlappenden Namespaces

Wenn Sie private und öffentliche gehostete Zonen mit überlappenden Namespaces wie „example.com“ und „accounting.example.com“ haben, leitet den Datenverkehr auf der Grundlage der spezifischsten Übereinstimmung weiter. Wenn Benutzer bei einer EC2-Instance in einer Amazon VPC angemeldet sind, die Sie der privaten gehosteten Zone zugeordnet haben, verarbeitet Route 53 Resolver DNS-Abfragen folgendermaßen:

1. bewertet, ob der Name der privaten gehosteten Zone dem Domänennamen in der Anforderungen entspricht, z. B. "finanzen.beispiel.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 die Anforderung an einen öffentlichen DNS-Auflöser weiter, und Ihre Anforderung wird als reguläre DNS-Abfrage aufgelöst.

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 private gehostete Zone gibt, aber keinen Datensatz, der dem Domänennamen und -typ in der Anforderung entspricht, leitet die Anforderung nicht an den 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 mindestens zwei private gehostete Zonen mit überlappenden Namespaces wie „example.com“ und „accounting.example.com“ verfügen, leitet den Datenverkehr auf der Grundlage der spezifischsten Übereinstimmung weiter.

> **Note**
>
> Wenn Sie über eine private gehostete Zone (example.com) und eine Route 53-Regel verfügen, die Datenverkehr für denselben Domänennamen an Ihr Netzwerk weiterleitet, hat die Resolver-Regel Vorrang. Siehe Private hosted zones and Route 53 Resolver rules.

Wenn Benutzer bei einer EC2-Instance in einer Amazon VPC angemeldet sind, die Sie allen privaten gehosteten Zonen zugeordnet haben, verarbeitet DNS-Abfragen folgendermaßen:

1. bewertet, ob der Domänenname in der Anforderung wie „accounting.example.com“ dem Namen einer der privaten gehosteten Zonen entspricht.
2. Wenn keine gehostete Zone vorhanden ist, die genau dem Domänennamen in der Anforderung entspricht, sucht nach einer gehosteten Zone mit einem Namen, der der übergeordnete Domänenname in der Anforderung 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`

Resolver wählt `accounting.example.com` aus, weil es spezifischer ist als `example.com`.

3. Resolver durchsucht die `accounting.example.com` gehostete Zone nach einem Datensatz, der dem Domänennamen und DNS-Typ in der Anforderung entspricht, z. B. einem A-Eintrag für `seattle.accounting.example.com`.

   Wenn kein Datensatz vorhanden ist, der dem Domänennamen und dem Typ in der Anforderung entspricht, gibt NXDOMAIN (nicht existierende Domäne) an den Client zurück.

Private gehostete Zonen und Route 53 Resolver-Regeln

Wenn Sie über eine private gehostete Zone (example.com) und eine -Regel verfügen, die Datenverkehr für denselben Domänennamen an Ihr Netzwerk weiterleitet, hat die -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-Regel, die Datenverkehr für example.com an Ihr Netzwerk weiterleitet, und Sie ordnen die Regel derselben VPC zu.

In dieser Konfiguration hat die -Regel Vorrang vor der privaten gehosteten 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 keine NS-Datensätze in einer privat gehosteten Zone erstellen, um die Verantwortlichkeit für eine Subdomäne zu delegieren.

Benutzerdefinierte DNS-Server

Wenn Sie benutzerdefinierte DNS-Server auf den Amazon-EC2-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 resolver verwenden. Weitere Informationen finden Sie unter Was ist? Amazon Route 53 Resolver.

Erforderliche IAM-Berechtigungen

Zum Erstellen von privat gehosteten Zonen müssen Sie IAM-Berechtigungen für Amazon EC2-Aktionen zusätzlich zu den Berechtigungen für Route 53-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 Domäne, die Sie in einer oder mehreren Amazon Virtual Private Clouds (VPCs) hosten. Sie erstellen eine gehostete Zone für eine Domäne (z. B. "example.com") und erstellen dann Datensätze, um Amazon Route 53 mitzuteilen, wie der Datenverkehr innerhalb und zwischen Ihren VPCs für diese Domäne weitergeleitet werden soll.

> **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 gehostete Zone erstellt haben, können Sie ihr weitere VPCs zuordnen, einschließlich VPCs, die Sie mit einem anderen AWS Konto erstellt haben.
> Um VPCs zuzuordnen, die Sie mit einem Konto mit einer privat gehosteten Zone erstellt haben, die mit einem anderen Konto erstellt wurde, 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 unter ListHostedZonen in der Amazon Route 53-API-Referenz.

Um die Hosting-Zonen aufzulisten, die einem AWS Konto zugeordnet sind

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

Zuordnen von weiteren VPCs zu einer privaten gehosteten Zone

Sie können die Amazon Route 53-Konsole verwenden, um mehr VPCs einer privaten Hosting-Zone zuzuordnen, wenn Sie die Hosting-Zone und die VPCs mit demselben AWS Konto erstellt haben.

> **Important**
>
> Um VPCs zuzuordnen, die Sie mit einem Konto mit einer privat gehosteten Zone erstellt haben, die mit einem anderen Konto erstellt wurde, müssen Sie zuerst die Zuordnung autorisieren. Darüber hinaus können Sie die AWS -Konsole nicht verwenden, um die Zuordnung zu autorisieren oder um die VPCs der gehosteten Zone zuordnen. Weitere Informationen finden Sie unter Zuordnen einer Amazon VPC und einer privaten gehosteten Zone, die Sie mit verschiedenen Konten erstellt haben AWS.

Informationen dazu, wie Sie mithilfe der Route 53-API mehr VPCs einer privaten Hosting-Zone zuordnen können, finden Sie unter AssociateVPC WithHosted Zone in der Amazon Route 53-API-Referenz.

So verknüpfen Sie zusätzliche VPCs mithilfe der Route 53-Konsole mit einer privat gehosteten Zone

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Aktivieren Sie das Optionsfeld für die privat gehostete Zone, der Sie mehrere VPCs zuordnen möchten.
4. Wählen Sie Edit (Bearbeiten).
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 mehrere VPCs mit dieser gehosteten Zone zu verknüpfen, 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 Weitere Informationen finden Sie unter create-vpc-association-authorizationAWS CLI in der Befehlsreferenz.
   - AWS SDK oder AWS Tools for Windows PowerShell— Weitere Informationen finden Sie in der entsprechenden Dokumentation auf der AWS Dokumentationsseite
   - Amazon Route 53-API — Weitere Informationen finden Sie unter CreateVPC AssociationAuthorization in der Amazon Route 53-API-Referenz

   Beachten Sie Folgendes:

- Wenn Sie mehrere VPCs, die Sie mit einem VPC-Konto erstellt haben, mit einer privat gehosteten Zone verknüpfen möchten, die Sie mit einem anderen Konto erstellt haben, müssen Sie für jede VPC eine Autorisierungsanforderung stellen.
- 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 Verknüpfung 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 Aktion WithHostedAssociateVPC Zone.
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.

> **Note**
>
> Informationen zur maximalen Anzahl der Autorisierungen, die Sie erstellen können, finden Sie unter Kontingente für Entitäten.

Aufheben der Verknüpfung von VPCs mit einer privaten gehosteten Zone

Sie können die Amazon Route 53-Konsole verwenden, um die Zuordnung von VPCs zu einer privat gehosteten Zone aufzuheben. 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.

So heben Sie die Verknüpfung von VPC mit einer privat gehosteten Zone auf

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
3. Wählen Sie die privat gehostete Zone aus, von der Sie eine oder mehrere VPCs trennen möchten.
4. Wählen Sie Edit (Bearbeiten).
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
- Löschen einer privat gehosteten Zone mit der Route 53-Konsole.

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 AWS Cloud Map bei der 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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.

Migrieren einer gehosteten Zone zu einem anderen AWS Konto

Wenn Sie eine gehostete Zone von einem AWS Konto zu einem anderen Konto migrieren möchten, können Sie die Datensätze in der alten gehosteten Zone programmgesteuert auflisten, die Ausgabe bearbeiten und dann mithilfe der bearbeiteten Ausgabe programmgesteuert Datensätze in einer neuen gehosteten Zone erstellen. Beachten Sie Folgendes:

- Wenn Sie nur wenige Datensätze haben, können Sie auch mit der Route 53-Konsole Datensätze in der neuen gehosteten Zone generieren. Weitere Informationen finden Sie unter Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole.
- Einige Prozeduren verwenden die AWS Command Line Interface (AWS CLI). Sie können diese Verfahren auch mithilfe eines der - AWS SDKs , der Amazon Route 53-API oder durchführen AWS Tools for Windows PowerShell. Für dieses Thema verwenden wir , AWS CLI da es für eine kleine Anzahl von gehosteten Zonen einfacher ist.
- Sie können dieses Verfahren auch anwenden, um Datensätze in einer neuen gehosteten Zone zu erstellen, die einen anderen Namen trägt als die vorhandene gehostete Zone, aber dieselben Datensätze enthält.
- Es ist nicht möglich, Alias-Datensätze zu migrieren, die Datenverkehr zu Datenverkehrsrichtlinien-Instances weiterleiten.

Themen

- Schritt 8: Aktualisieren der Domänenregistrierung, sodass die Nameserver für die neue gehostete Zone verwendet werden
- Schritt 9: Warten, bis DNS-Resolver die neue gehostete Zone verwenden
- Schritt 10: Löschen der alten gehosteten Zone (optional)

Schritt 1: Installieren oder Aktualisieren der AWS CLI

Informationen zum Herunterladen, Installieren und Konfigurieren der AWS CLIfinden Sie im AWS Command Line Interface -Benutzerhandbuch.

> **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.

Schritt 2: Erstellen der neuen gehosteten Zone

Das folgenden Verfahren erläutert, wie Sie mit der Route 53-Konsole die gehostete Zone erstellen, zu der Sie migrieren möchten.

> **Note**
>
> Route 53 weist eine neue Gruppe von vier Nameservern zur neuen gehosteten Zone zu. Nachdem Sie eine gehostete Zone zu einem anderen AWS Konto migriert haben, müssen Sie die Domänenregistrierung aktualisieren, um die Namenserver für die neue gehostete Zone zu verwenden. Wir erinnern Sie zu einem späteren Zeitpunkt im Prozess an diesen Schritt.

So erstellen Sie die neue gehostete Zone mit einem anderen Konto

1. Melden Sie sich bei der an AWS Management Console 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.

Schritt 3: Erstellen einer Datei mit den zu migrierenden Datensätzen

Erstellen Sie zum Migrieren von Datensätzen von einer gehosteten Zone zu einer anderen eine Datei mit den zu migrierenden Datensätzen, bearbeiten Sie die Datei und nutzen Sie diese dann, um Datensätze in der neuen gehosteten Zone zu erstellen. Gehen Sie wie folgt vor, um die Datei zu erstellen.

So erstellen Sie eine Datei, die die zu migrierenden Datensätze enthält

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Route-53-Konsole unter https://console.aws.amazon.com/route53/.

   Melden Sie sich mit den Anmeldeinformationen für das Konto an, das die gehostete Zone erstellt hat, die Sie migrieren möchten.
2. Rufen Sie die ID der gehostete Zone ab, die Sie migrieren möchten:

   a. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

   b. Suchen Sie die gehostete Zone, die Sie migrieren möchten. Wenn Sie viele gehostete Zonen haben, können SieGenauer Domänennameund geben Sie den Namen der gehosteten Zone ein, und drücken SieGeben Sie ein., um die Liste zu filtern.

   c. Rufen Sie den Wert der Spalte Hosted zone ID (ID der gehosteten Zone) ab.
3. 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 die ID der *hosted-zone-id*gehosteten Zone an, die Sie in Schritt 2 dieses Verfahrens erhalten haben.
- *path-to-output-file*Geben Sie für den Verzeichnispfad und den Dateinamen an, in dem Sie die Ausgabe speichern möchten.
- Das >-Zeichen sendet die Ausgabe an die angegebene Datei.
- Die übernimmt AWS CLI automatisch die Paginierung für gehostete Zonen, die mehr als 100 Datensätze enthalten. Weitere Informationen finden Sie unter Verwenden der Paginierungsoptionen der - AWS Befehlszeilenschnittstelle im AWS Command Line Interface - Benutzerhandbuch.

  Wenn Sie eine andere programmatische Methode verwenden, um Datensätze aufzulisten, z. B. eines der - AWS SDKs, können Sie maximal 100 Datensätze pro Ergebnisseite erhalten. Wenn die gehostete Zone mehr als 100 Datensätze enthält, müssen Sie mehrere Anforderungen zur Auflistung aller Datensätze übermitteln.
- Verwenden Sie die folgende Syntax, um den Befehl in Windows-Versionen PowerShell vor 6.0 auszuführen:

  ```
  aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
  ```

Wenn Sie beispielsweise AWS CLI auf einem Windows-Computer ausführen, können Sie den folgenden Befehl ausführen:

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp\list-records-ZOLDZONE12345.txt
```

Wenn Sie die AWS CLI auf einem Windows-Computer in einer Windows-Version PowerShell vor 6.0 ausführen, können Sie den folgenden Befehl ausführen:

```
$output = aws route53 list-resource-record-sets --hosted-zone-id <hosted-zone-id>;
 $mypath = <output-path ;
```

```
[System.IO.File]::WriteAllLines($mypath,$output)
```

4. Erstellen Sie eine Kopie dieser Ausgabe. Nachdem Sie Datensätze in der neuen gehosteten Zone erstellt haben, empfehlen wir Ihnen, den AWS CLI `list-resource-record-sets` Befehl in der neuen gehosteten Zone auszuführen und die beiden Ausgaben zu vergleichen, um sicherzustellen, dass alle Datensätze erstellt wurden.

Schritt 4: Bearbeiten der Datensätze, die Sie migrieren möchten

Das Format der Datei, die Sie im vorherigen Verfahren erstellt haben, entspricht dem Format, das für den AWS CLI `change-resource-record-sets` Befehl erforderlich ist, mit dem Sie Datensätze in der neuen gehosteten Zone erstellen. Für die Datei sind jedoch einige Änderungen erforderlich. Sie müssen einige der Änderungen auf jeden Datensatz anwenden. Sie können diese Änderungen mithilfe der Suchen- und Ersetzen-Funktion eines Text-Editors vornehmen.

Öffnen Sie eine Kopie der Datei, die Sie in Schritt 3: Erstellen einer Datei mit den zu migrierenden Datensätzen erstellt haben, und nehmen Sie die folgenden Änderungen vor:

- Löschen Sie die ersten beiden Zeilen oben in der Ausgabe:

```
{
    "ResourceRecordSets": [
```

- Löschen Sie die Zeilen, die sich auf NS- und SOA-Datensätze beziehen. Die neue gehostete Zone verfügt bereits über diese Datensätze.
- Optional – Fügen Sie ein `Comment`-Element hinzu.
- Fügen Sie ein `Changes`-Element hinzu.
- Fügen Sie für jeden Datensatz ein `Action`- und ein `ResourceRecordSet`-Element hinzu.
- Fügen Sie bei 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. Führen Sie eine Internet-Suche nach "`json validator`" durch, um einen Online-JSON-Validator zu finden.

- 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 Aliasdatensatz auf eine andere Ressource verweist, z. B. einen Load Balancer, ändern Sie die ID der gehosteten Zone nicht in die ID der gehosteten Zone der Ressource selbst, nicht in die ID der gehosteten Zone der Domain. Wenn Sie versehentlich die ID der gehosteten Zone ändern, setzen Sie die ID der gehosteten Zone auf die ID der gehosteten Zone der Ressource selbst zurück, nicht auf die ID der gehosteten Zone der Domain. Diese ID der gehosteten Zone finden Sie 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.
- Sie können diese Vorgehensweise verwenden, um Datensätze in einer gehosteten Zone zu erstellen, die einen anderen Namen trägt. Ändern Sie für jeden Datensatz in der Ausgabe den Teil des Domänennamens des `Name`-Elements in den Namen der neuen gehosteten Zone. Wenn Sie zum Beispiel Datensätze in der gehosteten Zone "example.com" auflisten und Datensätze in einer gehosteten Zone namens "example.net" erstellen möchten, ändern Sie den example.com-Teil eines jeden Datensatznamens in "example.net":

  From:

  - `"Name": "example.com."`

- "Name": "www.example.com."

auf:

- "Name": "example.net."
- "Name": "www.example.net."

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."
```

```
            }
        }
    ]
}
```

Schritt 5: Aufteilen großer Dateien in kleinere Dateien

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. Dies sind die Höchstwerte:

- Eine Datei darf maximal 1 000 Datensätze enthalten.
- Die maximale Gesamtlänge der Werte in allen `Value`-Elementen ist auf 32 000 Byte begrenzt.

Schritt 6: Erstellen von Datensätzen in der neuen gehosteten Zone

Verwenden Sie den folgenden AWS CLI Befehl, um Datensätze in der neuen gehosteten Zone zu erstellen:

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-new-hosted-zone --
change-batch file://path-to-file-that-contains-records
```

Beispielsweise:

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch
 file://c:/temp/change-records-ZNEWZONE1245.txt
```

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 7: Vergleichen von Datensätzen der neuen und alten gehosteten Zone

Zur Bestätigung, dass alle Datensätze erfolgreich in der neuen gehosteten Zone erstellt wurden, sollten Sie die Datensätze in der neuen gehosteten Zone auflisten und die Ausgabe mit der Liste der Datensätze der alten gehosteten Zone vergleichen. In diesem Fall verfahren Sie wie nachfolgend beschrieben.

So vergleichen Sie Datensätze der alten und neuen gehosteten Zone

1. Führen Sie den folgenden Befehl aus:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json
    > path-to-output-file
   ```

   Geben Sie die folgenden Werte an:

   - *hosted-zone-id*Geben Sie für die ID der neuen gehosteten Zone an.
   - *path-to-output-file*Geben Sie für 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 3: Erstellen einer Datei mit den zu migrierenden Datensätzen zugewiesen haben. Wenn Sie einen anderen Dateinamen nehmen, ist sichergestellt, dass die neue Datei die alte nicht überschreibt.
   - Das >-Zeichen sendet die Ausgabe an die angegebene Datei.

   Beispiel: Wenn Sie einen Windows-Computer verwenden, können Sie den folgenden Befehl ausführen:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json
    > c:\temp\list-records-ZNEWZONE67890.txt
   ```

2. Vergleichen Sie die Ausgabe mit der Ausgabe von Schritt 3: Erstellen einer Datei mit den zu migrierenden Datensätzen.

   Abgesehen von den Werten für die NS- und SOA-Datensätze und der Änderungen, die Sie in Schritt 4: Bearbeiten der Datensätze, die Sie migrieren möchten vorgenommen haben (z. B. unterschiedliche IDs der gehosteten Zonen oder Domänennamen), sollten beide Ausgaben identisch sein.

3. Wenn die Datensätze in der neuen gehosteten Zone nicht mit den Datensätzen in der alten gehosteten Zone übereinstimmen, können Sie einen der folgenden Schritte ausführen:

   - Nehmen Sie kleinere Korrekturen über die Route 53-Konsole vor. Weitere Informationen finden Sie unter Bearbeiten von Datensätzen.

- Fehlt eine große Anzahl von Datensätzen, erstellen Sie eine neue Textdatei, die die fehlenden Datensätze enthält, und wiederholen Sie Schritt 6: Erstellen von Datensätzen in der neuen gehosteten Zone.
- Löschen Sie alle Datensätze mit Ausnahme der NS- und SOA-Datensätze in der neuen gehosteten Zone und wiederholen Sie die folgenden Schritte:
  - Schritt 4: Bearbeiten der Datensätze, die Sie migrieren möchten
  - Schritt 5: Aufteilen großer Dateien in kleinere Dateien
  - Schritt 6: Erstellen von Datensätzen in der neuen gehosteten Zone
  - Schritt 7: Vergleichen von Datensätzen der neuen und alten gehosteten Zone

Schritt 8: Aktualisieren der Domänenregistrierung, sodass die Nameserver für die neue gehostete Zone verwendet werden

Wenn Sie das Erstellen der Datensätze in der neuen gehosteten Zone abgeschlossen haben, ändern Sie die Nameserver für die Domänenregistrierung, damit die Nameserver für die neue gehostete Zone verwendet werden.

> **Important**
>
> Wenn Sie die Domänenregistrierung nicht für die Verwendung der Nameserver für die neue gehostete Zone aktualisieren, verwendet Route 53 weiterhin die alte gehostete Zone zum Weiterleiten von Datenverkehr für die Domäne. Wenn Sie die alte gehostete Zone löschen, ohne Nameserver für die Domänenregistrierung zu aktualisieren, ist die Domäne im Internet nicht mehr erreichbar. Wenn Sie Datensätze in der neuen gehosteten Zone hinzufügen, aktualisieren oder löschen, ohne Nameserver für die Domänenregistrierung zu aktualisieren, wird der Datenverkehr nicht basierend auf diesen Änderungen umgeleitet.

Weitere Informationen finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

> **Note**
>
> Unabhängig davon, ob Sie das Verfahren zum Migrieren eines DNS-Services für eine Domäne nutzen, die sich in Verwendung befindet, oder das Verfahren für eine inaktive

Domäne, sie können in jedem Fall die folgenden Schritte überspringen, da Sie bereits eine neue gehostete Zone und die Datensätze in der Zone erstellt haben:

- Schritt 1: Abrufen der aktuellen DNS-Konfiguration vom aktuellen DNS-Serviceanbieter
- Schritt 2: Erstellen einer gehosteten Zone
- Schritt 3: Erstellen von Datensätzen

Schritt 9: Warten, bis DNS-Resolver die neue gehostete Zone verwenden

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 bis zu zwei Tage gespeichert.

Note

Wenn Sie Datensätze in der neuen gehosteten Zone erstellt haben, die nicht in der alten gehosteten Zone angezeigt wird, können die Benutzer die neuen Datensätze nicht für den Zugriff auf Ihre Ressourcen verwenden, bis die Resolver die Nameserver für die neue gehostete Zone verwenden. Angenommen, Sie erstellen den Datensatz "test.example.com" in der neuen gehosteten Zone, die Internetdatenverkehr an Ihre Website weiterleiten soll. Wenn der Datensatz nicht in der alten gehosteten Zone erscheint, kann "test.example.com" nicht in einem Webbrowser eingegeben werden, bis Resolver mit der Verwendung der neuen gehosteten Zone beginnen.

Um sicherzustellen, dass die Migration einer gehosteten Zone zu einem anderen AWS Konto abgeschlossen ist, bevor Sie die alte gehostete Zone löschen, warten Sie zwei Tage, nachdem Sie die Domänenregistrierung aktualisiert haben, um Namenserver für die neue gehostete Zone zu verwenden. Nachdem die zweitägige TTL abgelaufen ist und die Resolver den Nameserver für Ihre Domäne anfordern, rufen die Resolver die aktuellen Nameserver ab. Sie können auch Abfrageprotokollierung aktivieren, um die Abfragen in den neuen gehosteten Zonen zu überwachen. Weitere Informationen zu den Preisen für die Resolver-Abfrageprotokollierung finden Sie unter CloudWatch -Preise.

Schritt 10: Löschen der alten gehosteten Zone (optional)

Wenn Sie sicher sind, die alte gehostete Zone nicht mehr zu benötigen, können Sie diese löschen.

> **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.

Die gehostete Zone muss abgesehen von den standardmäßigen NS- und SOA-Datensätzen leer sein. Wenn die alte gehostete Zone viele Datensätze enthält, kann das Löschen mit der Konsole sehr lange dauern. Eine mögliche Option ist das Ausführen folgender Schritte:

1. Machen Sie eine weitere Kopie der bearbeiteten Datei aus Schritt 4: Bearbeiten der Datensätze, die Sie migrieren möchten.
2. Ändern Sie in der Kopie für jeden Datensatz `"Action": "CREATE"` in `"Action": "DELETE"`.
3. Verwenden Sie den folgenden AWS CLI Befehl, um die Datensätze zu löschen:

   ```
   aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --
   change-batch file:///path-to-file-that-contains-records
   ```

   > **Important**
   >
   > Stellen Sie sicher, dass der Wert, den Sie für die ID der gehosteten Zone angeben, die ID der alten gehosteten Zone und nicht die der neuen ist.

4. Löschen Sie alle verbliebenden Datensätze und die gehostete Zone:

   a. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Route-53-Konsole unter https://console.aws.amazon.com/route53/.

      Melden Sie sich mit den Anmeldeinformationen für das Konto an, über das die alte gehostete Zone erstellt wurde.

b. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

c. Wählen Sie den Namen der alten gehosteten Zone aus. Wenn Sie viele gehostete Zonen haben, können Sie Exact domain name (Genauer Domänenname) auswählen und geben Sie den Namen der gehosteten Zone ein, und drücken Sie die Eingabetaste, um die Liste zu filtern.

d. Wenn die gehostete Zone andere Datensätze als die standardmäßigen NS- und SOA-Datensätze enthält (z. B. Alias-Datensätze, die Datenverkehr zu einer Datenverkehrsrichtlinien-Instance umleiten), aktivieren Sie die entsprechenden Kontrollkästchen und wählen Delete Record Set (Datensatz löschen) aus.

e. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).

f. Wählen Sie in der Liste der gehosteten Zonen das Optionsfeld für die gehostete Zone aus, die Sie löschen möchten.

g. Wählen Sie Löschen.

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 visuellen Editor für Datenverkehrsfluss 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 Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr.

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
- Wählen zwischen Alias- und Nicht-Alias-Datensätzen
- Unterstützte DNS-Datensatztypen
- Erstellen von Datensätzen mithilfe der Amazon-Route-53-Konsole
- Berechtigungen für Ressourcendatensätze
- Werte, die Sie beim Erstellen oder Bearbeiten von Amazon Route 53-Datensätzen angeben
- Erstellen von Datensätzen durch Importieren einer Zonendatei
- Bearbeiten von Datensätzen
- Löschen von Datensätzen
- Auflisten von Datensätzen

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 Amazon EC2 EC2-Benutzerhandbuch.

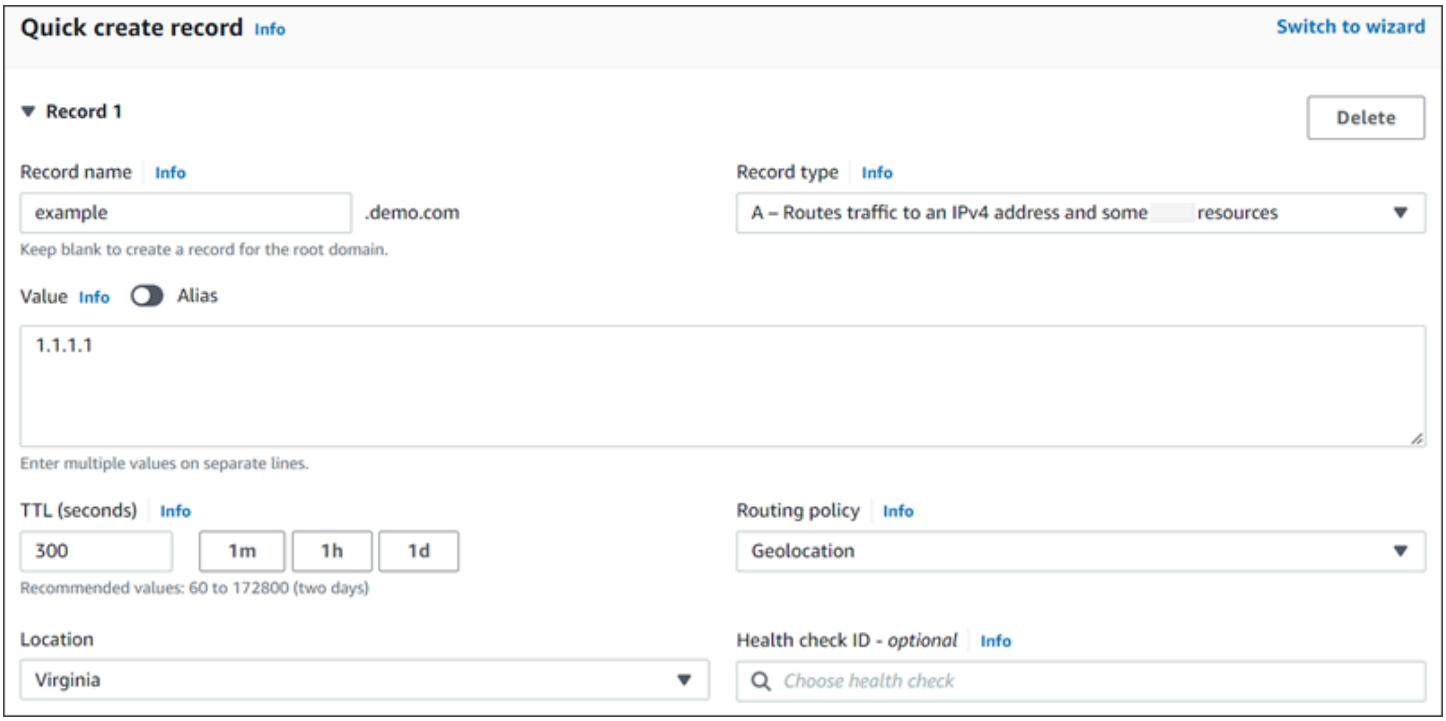
Wenn die DNS-Abfrage von einem On-Premises-Teil eines Hybridnetzwerks stammt, wird davon ausgegangen, dass sie aus der AWS-Region stammt, in der sich die VPC befindet.

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.



Routing mit Geoproximität

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.

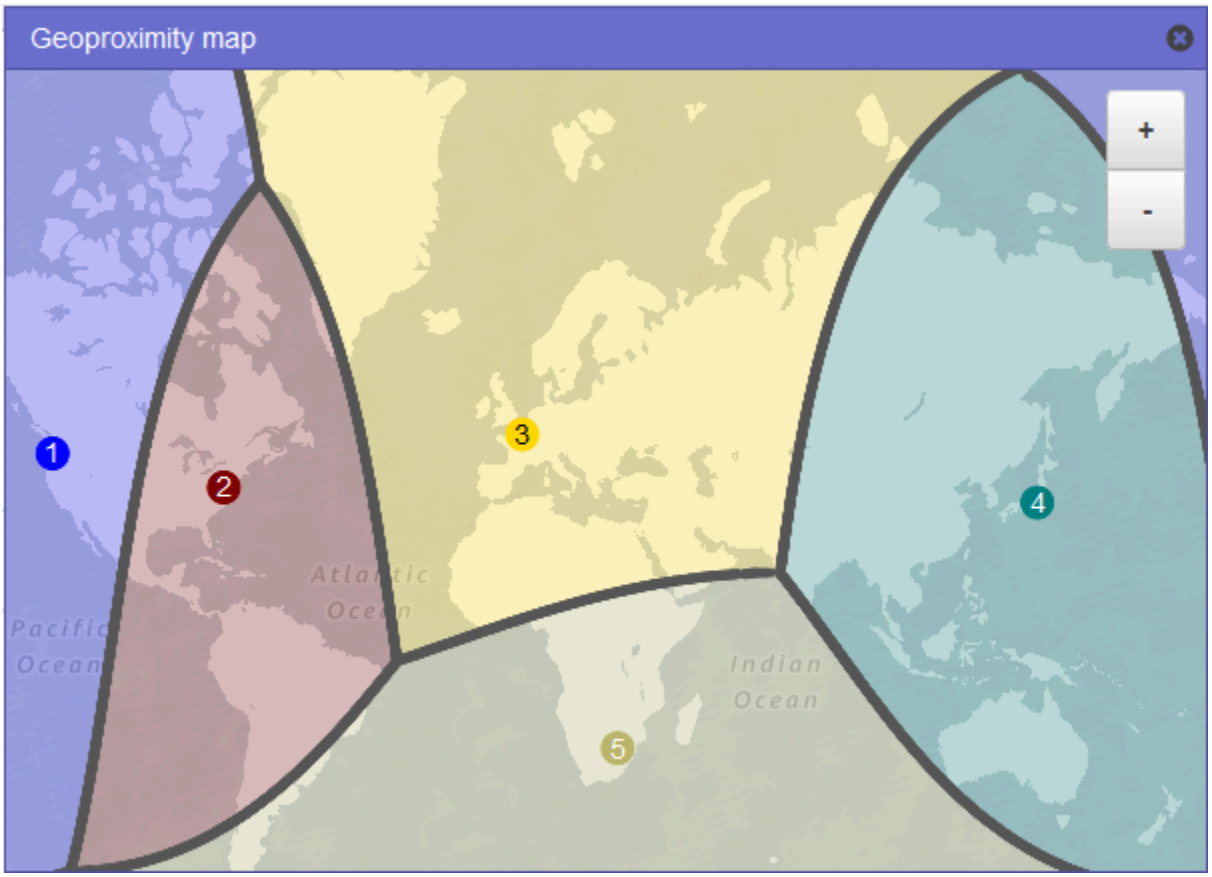
Weitere Informationen zum Unterschied zwischen AWS-Regionen und Local Zones finden Sie unter Regionen und Zonen im Amazon EC2 EC2-Benutzerhandbuch.

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:

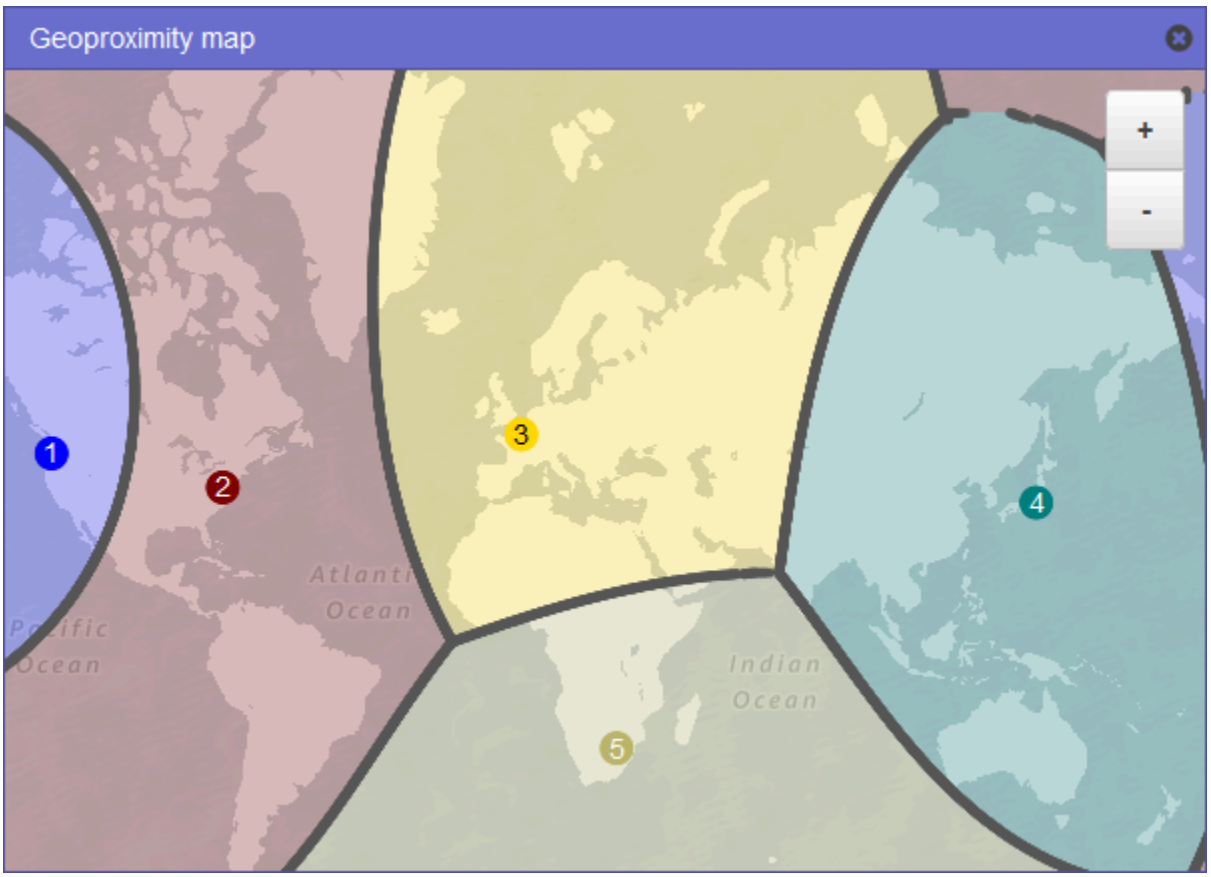
- Um die Größe der geografischen Region zu erweitern, aus der Route 53 Datenverkehr an eine Ressource weiterleitet, geben Sie für den Bias-Wert eine positive Ganzzahl von 1 bis 99 an. Route 53 verkleinert die Größe der angrenzenden Regionen.
- Um die Größe der geografischen Region zu verkleinern, aus 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.

Die folgende Karte zeigt vier AWS-Regionen (nummeriert von 1 bis 4) und einen Standort in Johannesburg, Südafrika, der nach Breiten- und Längengrad (5) spezifiziert ist.

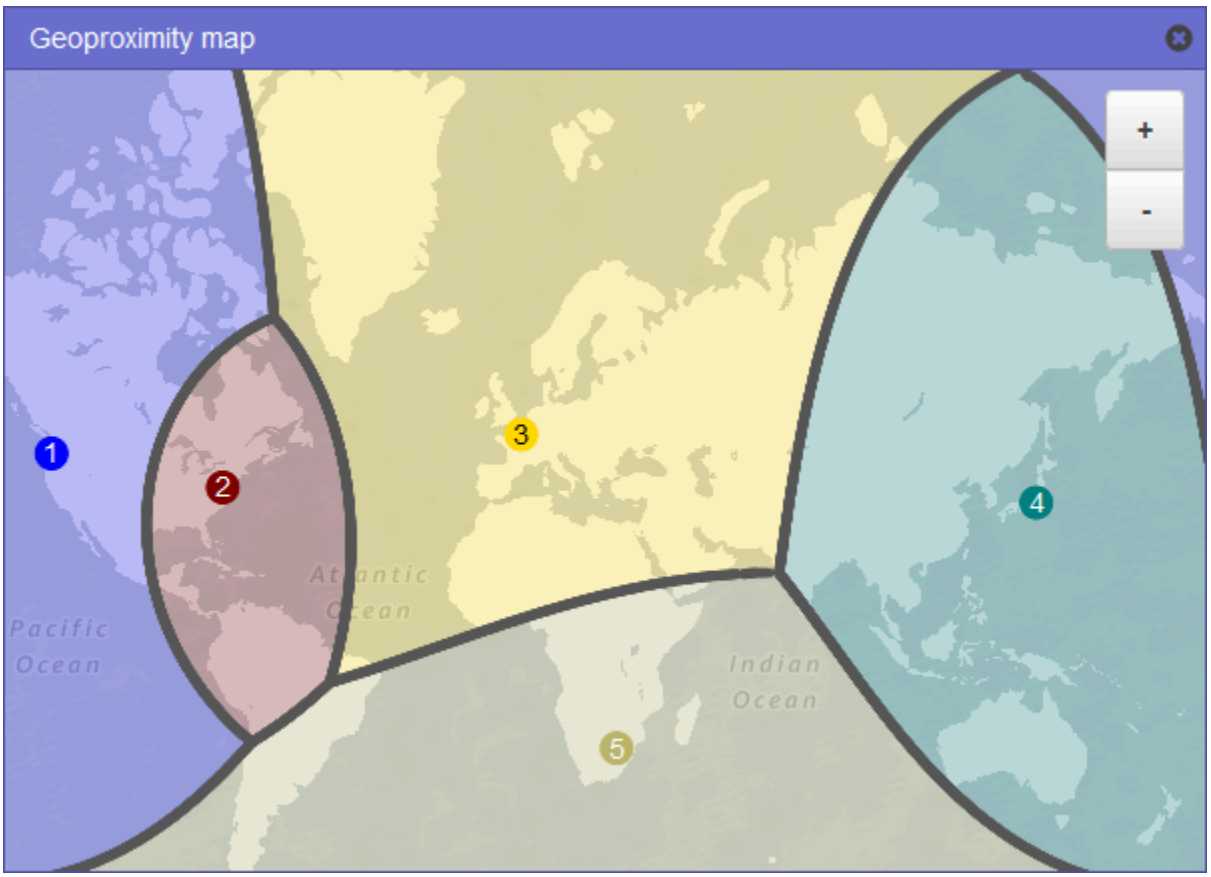
> **Note**
>
> Die Karten sind nur mit Verkehrsfluss verfügbar.



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 Abweichung positiv ist, behandelt Route 53 die Quelle einer DNS-Abfrage und die Ressource, die Sie in einem Geoproximitätsdatensatz angeben (z. B. eine EC2-Instance 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

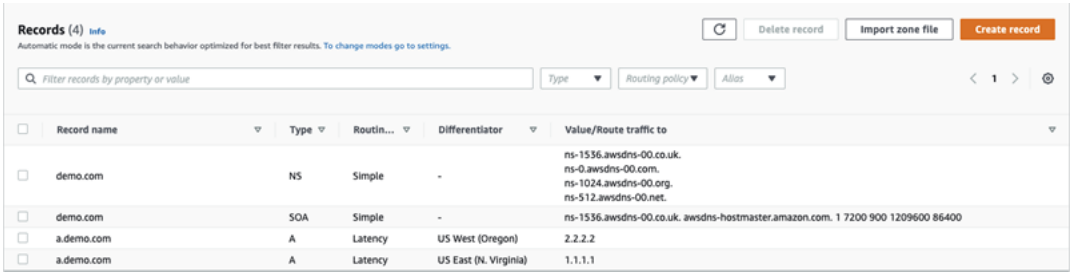
Latenzbasiertes Routing in privat gehosteten Zonen

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 gibt Ihnen eine detaillierte Kontrolle zur Optimierung der Leistung oder zur Senkung der Netzwerkkosten, indem Sie Ihre Daten in Form von User-IP-zu-Endpunkt-Zuordnungen auf Route 53 hochladen.

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 ISPs an bestimmte Endpunkte weiterleiten, um die Kosten oder die Leistung des Netztransitverkehrs 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.

Verwalten von IP-Bereichen und Zuordnung zu einem Ressourcendatensatz (RRSet)

Für IPv4 können Sie CIDR-Blöcke mit einer Länge zwischen 1 und 24 Bit verwenden, während Sie für IPv6 CIDR-Blöcke mit einer Länge zwischen 1 und 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 aus 2001:0DB8:0000:1234::/48 stammt, stimmt sie überein. Wenn Sie dagegen „2001:0DB8:0000:1234::/48“ in Ihrer CIDR-Sammlung angeben und eine Abfrage von „2001:0DB8::/32“ stammt, gibt es keine Übereinstimmung 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, z. B. 192.0.2.0/24 oder 2001:DB8::/32.

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:DB8: :/32]. Die Blöcke in einer CIDR-Standortliste müssen nicht benachbart sein oder über denselben Bereich verfügen.

Ein einzelner Standort kann sowohl IPv4- als auch IPv6-Blöcke haben und mit A- bzw. mit AAAA-Einträgen verknüpft 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 example-isp-seattle example-isp-tokyo mycollection = [,].

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 diese Sammlungen auch mit AWS RAM anderen AWS Konten teilen. Wenn Sie eine Aktualisierung vornehmen, z. B. die Bearbeitung eines IP-Bereichs in einer Sammlung, gilt diese Aktualisierung automatisch für alle Datensatzsätze, die mit der Sammlung verknüpft sind.

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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. Dies können IPv4- oder IPv6-Adressen von /0 bis /24 für IPv4 und /0 bis /48 für IPv6 sein.

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 Route 53-Konsole an AWS Management Console 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 Route 53-Konsole an AWS Management Console 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 z. B. `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 dies Schrittweise

durch Änderung der Gewichtungen 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	N/A
DNS-Abfrage beantwortet?	Ja	Ja	Nein
Status der Zustandsprüfung	Fehlerhaft	Fehlerhaft	N/A
DNS-Abfrage beantwortet?	Nein	Nein	Ja
Status der Zustandsprüfung	Fehlerhaft	Fehlerfrei	N/A
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 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 private gehostete Zonen verwendet Route 53 Daten von den Route 53-Resolvern, in denen sich die private gehostete Zone befindet AWS-Region , um Entscheidungen über Geolokalisierung und Latenzrouting zu treffen.

Weitere Informationen zu edns-client-subnet finden Sie im EDNS-Client-Subnetz-RFC, 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.
- 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 Accelerator.
- 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.

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 Geoproximity-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-Datensätzen können Sie mit Alias-Datensätzen Datenverkehr an ausgewählte AWS-Ressourcen, wie z. B. CloudFront-Verteilungen und Amazon-S3-Buckets, weiterleiten. Weitere Hinweise, einschließlich eines Vergleichs von Alias- und CNAME-Datensätzen, finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

A-Datensatztyp

Sie verwenden einen A-Datensatz, um Datenverkehr mit einer IPv4-Adresse in punktierter Dezimalnotation 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-Datensatz, um Datenverkehr an eine Ressource, z. B. einen Webserver, mithilfe einer IPv6-Adresse im durch Doppelpunkt getrennten Hexadezimalformat 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-Datensatz gibt an, welche Zertifizierungsstellen (Certificate Authorities, CAs) Zertifikate für eine Domäne oder Subdomäne ausgeben dürfen. Die Erstellung eines CAA Datensatzes hilft, zu verhindern, dass die falschen CAs Zertifikate für Ihre Domänen ausgeben. 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 (Certificate Authority, CAs) SSL/TLS-Zertifikate ausstellen können, falls überhaupt.
- 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 lassen 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

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"
```

Weitere Informationen dazu, wie Sie AWS Certificate Manager zum Ausstellen eines Zertifikats autorisieren, finden Sie unter Konfigurieren eines CAA-Datensatzes 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`
- Tag – `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`
- Tag – `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 Zertifizierungsstellen bekannt, 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-Verteilungen und Amazon-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>
```

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. Ein häufiges Beispiel ist die Konvertierung von Telefonnummern in SIP-URIs.

Das `Value`-Element für einen NAPTR-Datensatz besteht aus sechs durch Leerzeichen getrennten Werten:

Reihenfolge

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 der entsprechenden RFC-Dokumentation:

- URI-DDDS-Anwendung – https://tools.ietf.org/html/rfc3404#section-4.4
- S-NAPTR-DDDS-Anwendung – https://tools.ietf.org/html/rfc3958#section-6.5
- 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-Datensätzen finden Sie in den 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.

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) for Authorizing Use of Domains in Email, Version 1, wurde aktualisiert und besagt nun: "... die Existenz und Mechanismen in [RFC4408] 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>
```

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

Enthält Ihr TXT-Datensatz eines der folgenden Zeichen, müssen Sie die Zeichen durch Escape-Zeichen im Format *dreistelligen Oktalcode* angeben:

- 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 ein Mapping von 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 Editor für Datenverkehrsfluss 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 Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr.

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 zum Weiterleiten des Internetdatenverkehrs an Ihre Ressourcen, wie z. B. Amazon-S3-Buckets oder Amazon-EC2-Instances, finden Sie unter Erstellen 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 Datensätze der geografischen Nähe
- Spezifische Werte für Geoproximity-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 Management Console 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 Amazon EC2-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 AWS Management Console ab.
8. Melden Sie sich AWS Management Console 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 zu Ressourcendatensätzen finden Sie unter Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle zum Verwalten von Ressourcendatensätzen.

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 über die Amazon-Route-53-Konsole erstellen, hängen die Werte, die Sie angeben, davon ab, welche Routing-Richtlinie Sie verwenden möchten und ob Sie Aliasdatensätze erstellen, die den Datenverkehr an AWS-Ressourcen weiterleiten.

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 Domänennamen 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 – IPv6-Adresse

Eine IP-Adresse im IPv6-Format, zum Beispiel 2001:0db8:85a3:0:0:8a2e: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 (Certificate Authority, CAs) SSL/TLS-Zertifikate ausstellen können, falls überhaupt.
- 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-Verteilungen und Amazon-S3-Buckets

Der Wert, den Sie angeben, hängt zum Teil von der AWS-Ressource ab, an die Sie Verkehr weiterleiten:

- CloudFront-Verteilung – Ihre Verteilung muss einen alternativen Domänennamen enthalten, der dem Namen des Datensatzes entspricht. Wenn der Name des Datensatzes acme.example.com ist, muss die CloudFront-Verteilung acme.example.com als einen der alternativen Domänennamen beinhalten. Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen (CNAMEs) im Amazon-CloudFront-Entwicklerhandbuch.
- 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 Domänennamen 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, zu der Sie den Datenverkehr leiten.

Weitere Informationen zur Konfiguration von Route 53 zum Weiterleiten von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Important

Wenn Sie das gleiche AWS-Konto verwendet haben, um Ihre gehostete Zone und die Ressource zu erstellen, zu der Sie den Datenverkehr leiten, und Ihre Ressource nicht in der Liste Endpunkte aufgeführt ist, 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 Datenverkehr an einen S3 Bucket weiterzuleiten, müssen Sie A – IPv4-Adresse 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 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 zum erstellen der gehosteten Zone und der Ressource verschiedene AWS-Konten verwendet haben, wird die Ressource nicht in der Liste Endpunkt angezeigt. In der folgenden Dokumentation zu Ihrem Ressourcentyp erfahren Sie, welchen Wert Sie unter Endpunkt eingeben müssen.

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte APIs

Im Fall von benutzerdefinierten regionalen API-Gateway-APIs und Edge-optimierten APIs führen Sie Folgendes 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. Bei einer großen Anzahl von 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 für die Erstellung der aktuellen gehosteten Zone ein AWS-Konto und für die Erstellung einer API ein anderes Konto verwendet haben, wird die API nicht in der Liste Endpunkte unter API-Gateway-APIs angezeigt.

  Wenn Sie für die Erstellung der aktuellen gehosteten Zone ein Konto und für die Erstellung aller Ihrer APIs ein oder mehrere andere Konten verwendet haben, wird in der Liste Endpunkte Keine Ziele verfügbar unter API-Gateway-APIs angezeigt. Weitere Informationen finden Sie unter Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens.

CloudFront-Verteilungen

Führen Sie für CloudFront-Verteilungen einen der folgenden Schritte aus:

- Wenn Sie für die Erstellung Ihrer gehosteten Route-53-Zone und Ihrer CloudFront-Verteilung dasselbe Konto verwendet haben – Wählen Sie Endpunkt und eine Verteilung 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 Verteilung gerade eben einen alternativen Domänennamen hinzugefügt haben, kann es 15 Minuten dauern, bis Ihre Änderungen an alle CloudFront-Edge-Standorte propagiert wurden. Erst wenn die Änderungen propagiert wurden, kann Route 53 den neuen alternativen Domänennamen kennen.
- Wenn Sie unterschiedliche Konten verwendet haben, um Ihre gehostete Route-53-Zone und Ihre Verteilung zu erstellen – Geben Sie den CloudFront-Domänennamen für die Verteilung ein, z. B. d111111abcdef8.cloudfront.net.

  Wenn Sie für die Erstellung der aktuellen gehosteten Zone ein AWS-Konto und für die Erstellung einer Verteilung ein anderes Konto verwendet haben, wird die Verteilung nicht in der Liste Endpunkte angezeigt.

  Wenn Sie die für die Erstellung der aktuellen gehosteten Zone ein Konto und für die Erstellung aller Ihrer Verteilungen ein oder mehrere andere Konten verwendet haben, wird in der Liste Endpunkte Keine Ziele verfügbar unter CloudFront-Verteilungen angezeigt

> **Important**
>
> Leiten Sie keine Abfragen an eine CloudFront-Verteilung weiter, die nicht an alle Edge-Standorte propagiert wurde, da Ihre Benutzer in diesem Fall nicht auf die jeweiligen Inhalte zugreifen können.

Die CloudFront-Verteilung muss einen alternativen Domänennamen enthalten, der dem Namen des Datensatzes entspricht. Wenn der Name des Datensatzes acme.example.com ist, muss die CloudFront-Verteilung acme.example.com als einen der alternativen Domänennamen beinhalten.

Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen (CNAMEs) im Amazon-CloudFront-Entwicklerhandbuch.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse. Weitere Informationen finden Sie unter Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens.

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 Domänenname 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 in 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 für die Erstellung der aktuellen gehosteten Zone ein AWS-Konto und für die Erstellung eines Load Balancer ein anderes Konto verwendet haben, wird der Load Balancer nicht in der Liste Endpunkte 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 Domänennamen (example.com) oder Subdomänennamen (www.example.com) anfordert, kann der Client eine IPv4-Adresse (einen A-Datensatz), eine IPv6-Adresse (einen AAAA-Datensatz) oder sowohl die IPv4- als auch die IPv6-Adresse (in getrennten Anforderungen) 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 Global-Accelerator-Accelerators

Geben Sie für AWS-Global-Accelerator-Accelerators den DNS-Namen für den Accelerator ein. Sie können den DNS-Namen eines Accelerators eingeben, den Sie mit dem aktuellen AWS-Konto oder 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-Buckets ein anderes als das aktuelle AWS-Konto verwendet haben, wird der Bucket nicht in der Liste Endpunkte 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.

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 für die Erstellung Ihrer gehosteten Route-53-Zone und Ihres Schnittstellenendpunkts verschiedene Konten verwendet haben – 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 für die Erstellung der aktuellen gehosteten Zone ein AWS-Konto und für die Erstellung eines Schnittstellenendpunkts ein anderes Konto verwendet haben, wird der Schnittstellenendpunkt nicht in der Liste Endpunkte unter VPC-Endunkte 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 – IPv6-Adresse

- 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 AWS GovCloud (US) Region verwenden, unterliegt dieses Feature einigen 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 Datenverkehr leiten.

Informationen dazu, auf welche AWS-Ressourcen Sie abzielen können, finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen über die Konfiguration von Route 53 zum Weiterleiten von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Typ und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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.

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 – IPv6-Adresse

- 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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 jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Typ und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket.

Wählen Sie A – IPv4-Adresse aus.

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, zu der Sie den Datenverkehr leiten.

Informationen dazu, auf welche AWS-Ressourcen Sie abzielen können, finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 zum Weiterleiten von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung 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.

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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand bewerten nicht auf Jafestlegen, wenn es sich beim Endpunkt um eine CloudFront-Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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 – IPv6-Adresse
- 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 privat gehostete Zone den Kontinent, das Land oder die Unterabteilung aus, die der AWS-Region, in der sich Ihre Ressource befindet, am nächsten ist. 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. Wenn Sie den Standardspeicherort konfigurieren, legen Sie den Ländercode auf ein Sternchen „*“ fest.

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

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**
>
> Für die folgenden Länder bietet Route 53 keine Unterstützung zur Erstellung von Geolocation-Datensätzen: Bouvet-Insel (BV), Weihnachtsinsel (CX), Westsahara (EH) und Heard- und McDonald-Inseln (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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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
- Datensatzname
- Datensatztyp
- Bewerten/Weiterleiten des Datenverkehrs an
- Ort
- US-Staaten
- Zustandsprüfung
- Evaluate Target Health
- Datensatz-ID

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 jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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 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.

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 Datenverkehr leiten.

Weitere Informationen dazu, welche AWS-Ressourcen Sie markieren können, finden Sie unter Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 zum Weiterleiten von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

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 U.S. States (USA) aus.

Wählen Sie für eine privat gehostete Zone den Kontinent, das Land oder die Unterabteilung aus, die der AWS-Region, in der sich Ihre Ressource befindet, am nächsten ist. 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. Wenn Sie den Standardspeicherort konfigurieren, legen Sie den Ländercode auf ein Sternchen „*“ fest.

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

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

Für die folgenden Länder bietet Route 53 keine Unterstützung zur Erstellung von Geolocation-Datensätzen: Bouvet-Insel (BV), Weihnachtsinsel (CX), Westsahara (EH) und Heard- und McDonald-Inseln (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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand bewerten nicht auf Jafestlegen, wenn es sich beim Endpunkt um eine CloudFront-Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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 Datensätze der geografischen Nähe

Wenn Sie Datensätze zur geografischen Nähe 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 Datensätze der geografischen Nähe 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 von Datensätzen mit geografischer Nähe 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 – IPv6-Adresse
- 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 wie folgt angeben:

Benutzerdefinierte Koordinaten

Geben Sie den Längen- und Breitengrad für einen geopografischen Bereich an.

AWS-Region

Wählen Sie eine verfügbare Region aus der Liste Standort aus.

Weitere Informationen zu den -Regionen finden Sie unter AWS Globale Infrastruktur.

AWS Local Zone-Gruppe

Wählen Sie eine verfügbare Local-Zone-Gruppe aus der Liste Standort aus.

Weitere Informationen zu Local Zones finden Sie unter Verfügbare Local Zones im AWS Benutzerhandbuch für Local Zones. Eine lokale Zonengruppe ist normalerweise die lokale Zone ohne das Endzeichen. Wenn die Local Zone beispielsweise ist, ist `us-east-1-bue-1a` die Local Zone-Gruppe `us-east-1-bue-1`.

Sie können die Local Zones-Gruppe für eine bestimmte Local Zone auch mithilfe des describe-availability-zones CLI-Befehls identifizieren:

```
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 Folgendes zurück: `"GroupName": "us-west-2-den-1"`, was angibt, dass die Local Zone zur Local Zone-Gruppe `us-west-2-den-1a` gehört`us-west-2-den-1`.

Sie können keine Datensätze erstellen, die keine Geop-Unterbrechungsdatensätze haben, die die gleichen Werte für Datensatzname und Datensatztyp wie Datensätze mit geografischer Nähe haben.

Sie können auch nicht zwei Ressourcendatensätze für geografische Nähe erstellen, die denselben Speicherort für denselben Datensatznamen und Datensatztyp angeben.

Bias

Ein Bias erweitert oder verkleinert entweder einen geografischen Bereich, aus dem Route 53 Datenverkehr an eine Ressource weiterleitet. Eine positive Verzerrung erweitert die Fläche und eine negative Verzerrung verkleinert sie. 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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 Zielzustand bewerten für einen Aliasdatensatz oder die Datensätze in einer Gruppe von Failover-Alias, Geolocation-Alias, Geoproximitätsalias, Latenzalias, IP-basiertem Alias oder gewichtetem Aliasdatensatz 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 ein Endpunkt fehlerhaft ist, sucht Route 53 bei Datensätzen mit geografischer Nähe nach einem nächstgelegenen Endpunkt, der immer noch fehlerfrei ist.

Datensatz-ID

Geben Sie einen Wert ein, der diesen Datensatz in der Gruppe der Datensätze der geografischen Nähe eindeutig identifiziert.

Spezifische Werte für Geoproximity-Aliasdatensätze

Wenn Sie Alias-Datensätze für geografische Nähe erstellen, geben Sie die folgenden Werte an.

Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Themen

- Routing-Richtlinie
- Datensatzname
- Datensatztyp
- Bewerten/Weiterleiten des Datenverkehrs an
- Endpunktstandort
- Bias
- Zustandsprüfung
- Evaluate Target Health
- Datensatz-ID

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 Datensatzname keinen Wert ein (zum Beispiel ein @-Symbol).

Geben Sie denselben Namen für alle Datensätze in der Gruppe der Datensätze der geografischen Nähe ein.

Weitere Informationen über Datensatznamen finden Sie unter Datensatzname.

Datensatztyp

Der DNS-Datensatztyp. Weitere Informationen finden Sie unter Unterstützte DNS-Datensatztypen.

Wählen Sie den jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr weiterleiten. Wählen Sie denselben Wert für alle Datensätze in der Gruppe von Datensätzen mit geografischer Nähe 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 Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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 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.

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 Datenverkehr leiten.

Weitere Informationen dazu, welche AWS-Ressourcen Sie markieren können, finden Sie unter Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 zum Weiterleiten von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Endpunktstandort

Sie können den Speicherort des Ressourcenendpunkts wie folgt angeben:

Benutzerdefinierte Koordinaten

Geben Sie den Längen- und Breitengrad für einen geopografischen Bereich an.

AWS-Region

Wählen Sie eine verfügbare Region aus der Liste Standort aus.

Weitere Informationen zu den -Regionen finden Sie unter AWS Globale Infrastruktur.

AWS Local Zone-Gruppe

Wählen Sie eine verfügbare Region der lokalen Zone aus der Liste Standort aus.

Weitere Informationen zu Local Zones finden Sie unter Verfügbare Local Zones im AWS Benutzerhandbuch für Local Zones. Eine lokale Zonengruppe ist normalerweise die lokale Zone ohne das Endzeichen. Wenn die Local Zone beispielsweise ist, ist `us-east-1-bue-1a` die Local Zone-Gruppe `us-east-1-bue-1`.

Sie können die Local Zones-Gruppe für eine bestimmte Local Zone auch mit dem describe-availability-zones CLI-Befehl identifizieren:

```
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 Folgendes zurück: `"GroupName": "us-west-2-den-1"`, was angibt, dass die Local Zone zur Local Zone-Gruppe `us-west-2-den-1a` gehört`us-west-2-den-1`.

Sie können keine Datensätze erstellen, die nicht geoproximity sind und die dieselben Werte für Datensatzname und Datensatztyp wie Datensätze haben.

Sie können auch nicht zwei Ressourcendatensätze für geografische Nähe erstellen, die denselben Speicherort für denselben Datensatznamen und Datensatztyp angeben.

Weitere Informationen finden Sie unter available-local-zones.html.

Bias

Ein Bias erweitert oder verkleinert entweder einen geografischen Bereich, aus dem Route 53 Datenverkehr an eine Ressource weiterleitet. Eine positive Verzerrung erweitert die Fläche und eine negative Verzerrung verkleinert sie. 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten

Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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 Zielzustand bewerten für einen Aliasdatensatz oder die Datensätze in einer Gruppe von Failover-Alias, Geolocation-Alias, Geoproximitätsalias, Latenzalias, IP-basiertem Alias oder gewichtetem Aliasdatensatz 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 ein Endpunkt fehlerhaft ist, sucht Route 53 bei Datensätzen mit geografischer Nähe nach einem nächstgelegenen Endpunkt, der immer 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand 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 Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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 Datensätze der geografischen Nähe 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 – IPv6-Adresse
- 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 Amazon EC2-Region, in der sich die von Ihnen in diesem Datensatz angegebene Ressource befindet. Route 53 empfiehlt basierend auf anderen von Ihnen angegebenen Werten eine Amazon EC2-Region. Dies gilt auch für privat gehostete Zonen. Wir empfehlen, diesen Wert nicht zu ändern.

Beachten Sie Folgendes:

- Sie können für jede Amazon EC2-Region nur einen Latenzdatensatz erstellen.
- Es ist nicht notwendig, für alle Amazon EC2-Regionen Latenzdatensätze zu 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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
- Datensatzname
- Datensatztyp
- Bewerten/Weiterleiten des Datenverkehrs an
- Region
- Zustandsprüfung
- Evaluate Target Health
- Datensatz-ID

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 jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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 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.

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, zu der Sie den Datenverkehr leiten.

Informationen dazu, auf welche AWS-Ressourcen Sie abzielen können, finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 für die Weiterleitung von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Region

Die Amazon-EC2-Region, in der sich die von Ihnen in diesem Datensatz angegebene Ressource befindet. Route 53 empfiehlt basierend auf anderen von Ihnen angegebenen Werten eine Amazon EC2-Region. Dies gilt auch für privat gehostete Zonen. Wir empfehlen, diesen Wert nicht zu ändern.

Beachten Sie Folgendes:

- Sie können für jede Amazon EC2-Region nur einen Latenzdatensatz erstellen.
- Es ist nicht notwendig, für alle Amazon EC2-Regionen Latenzdatensätze zu 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand bewerten nicht auf Jafestlegen, wenn es sich beim Endpunkt um eine CloudFront-Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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 Domänennamen 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 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 – IPv6-Adresse
- 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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
- Ort
- Zustandsprüfung
- 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-Verteilungen und Amazon-S3-Buckets

Der Wert, den Sie angeben, hängt zum Teil von der AWS-Ressource ab, an die Sie Verkehr weiterleiten:

- CloudFront-Verteilung – Ihre Verteilung muss einen alternativen Domänennamen enthalten, der dem Namen des Datensatzes entspricht. Wenn der Name des Datensatzes acme.example.com ist, muss die CloudFront-Verteilung acme.example.com als einen der alternativen Domänennamen beinhalten. Weitere Informationen finden Sie unter Verwenden alternativer Domänennamen (CNAMEs) im Amazon-CloudFront-Entwicklerhandbuch.
- 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 Domänennamen 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 jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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 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.

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 Datenverkehr leiten.

Informationen dazu, auf welche AWS-Ressourcen Sie abzielen können, finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 für die Weiterleitung von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung des Internetverkehrs zu Ihren AWS Ressourcen.

Ort

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 Datensätze ohne IP-Basis erstellen, die über dieselben Werte wie IP-Basierte Datensätze für Datensatzname und Datensatztyp verfügen.

Weitere Informationen 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand bewerten nicht auf Jafestlegen, wenn es sich beim Endpunkt um eine CloudFront-Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-

Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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 – IPv6-Adresse
- 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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 – IPv6-Adresse
- 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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 jeweiligen Wert basierend auf der AWS-Ressource aus, an die Sie Datenverkehr 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-Verteilung

Wählen Sie A – IPv4-Adresse aus.

Wenn IPv6 für die Verteilung aktiviert ist, erstellen Sie zwei Datensätze: einen Datensatz mit dem Wert A – IPv4-Adresse als Datensatztyp und einen Datensatz mit dem Wert AAAA – IPv6-Adresse.

Elastic-Beanstalk-Umgebung, die über regionale Subdomänen verfügt

Wählen Sie A – IPv4-Adresse aus.

ELB-Load Balancer

Wählen Sie A – IPv4-Adresse oder AAAA – IPv6-Adresse aus.

Amazon-S3-Bucket

Wählen Sie A – IPv4-Adresse aus.

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 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.

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, zu der Sie den Datenverkehr leiten.

Informationen dazu, auf welche AWS-Ressourcen Sie abzielen können, finden Sie unter Gemeinsame Werte für Bewerten/Weiterleiten des Datenverkehrs an.

Weitere Informationen zur Konfiguration von Route 53 für die Weiterleitung von Datenverkehr an spezifische AWS-Ressourcen finden Sie unter Weiterleitung 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 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 prüfen den Zustand aller Datensätze in einer Gruppe von Datensätzen mit demselben Namen, demselben Typ und derselben Weiterleitungsrichtlinie (z. B. Failover- oder gewichteten Datensätzen) und geben für alle Datensätze Zustandsprüfungs-IDs 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:

Benutzerdefinierte regionale API-Gateway- und Edge-optimierte 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 Zielzustand bewerten nicht auf Jafestlegen, wenn es sich beim Endpunkt um eine CloudFront-Verteilung handelt.

Elastic Beanstalk-Umgebungen, die über regionale Subdomänen verfügen

Wenn Sie in Endpunkt eine Elastic-Beanstalk-Umgebung angeben und diese einen ELB-Load-Balancer enthält, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. (Eine Umgebung enthält automatisch einen ELB-Load Balancer, wenn sie mehr als eine Amazon EC2-Instance umfasst.) Wenn Sie Zielzustand bewerten auf Ja setzen und entweder keine fehlerfreien Amazon-EC2-Instances zur Verfügung stehen oder der Load Balancer selbst fehlerhaft ist, leitet Route 53 Abfragen an andere fehlerfreie Ressourcen weiter, sofern vorhanden.

Bei einer Umgebung, die nur eine einzelne Amazon EC2-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 Endpunkt einen ELB-Classic-Load-Balancer angeben, leitet Elastic Load Balancing Abfragen nur an die fehlerfreien Amazon-EC2-Instances weiter, die beim Load Balancer registriert sind. Wenn Sie Zielzustand bewerten auf Ja festlegen und es entweder keine fehlerfreien EC2-Instances gibt 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 die AWS-Ressource, die Sie in Endpunkt angeben, ein Datensatz oder eine Gruppe von Datensätzen (z. B. eine Gruppe von gewichteten Datensätzen), aber kein weiterer Alias-Datensatz ist, wird empfohlen, dass Sie eine Zustandsprüfung mit sämtlichen Datensätzen im Endpunkt verknüpfen. 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.
- 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.

Route 53 unterstützt das Exportieren von Datensätzen in eine Zonendatei nicht.

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.

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.
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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Save Changes (Änderungen speichern).
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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.

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.

In diesem Kapitel wird erläutert, wie Sie die DNSSEC-Signatur für Route 53 aktivieren, wie Sie mit Schlüsselsignierungsschlüsseln (KSKs) arbeiten und Probleme beheben. Sie können mit der DNSSEC-Signatur in der AWS Management Console oder programmgesteuert mit der -API arbeiten. Weitere Informationen zur Verwendung der CLI oder SDKs für die Verwendung von Route 53 finden Sie unter Amazon 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. Wir empfehlen dringend, einen CloudWatch Alarm einzurichten, der Sie benachrichtigt, wenn ein -`DNSSECInternalFailure` oder -`DNSSECKeySigningKeysNeedingAction`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.

Themen

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

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. 200202240 1 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 GetChange, um sicherzustellen, dass Ihre Änderungen bisher 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) mithilfe von AWS CLI oder in der Route-53-Konsole erstellen.

- CLI
- Konsole

Wenn Sie einen vom Kunden verwalteten KMS-Schlüssel bereitstellen oder erstellen, gelten 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, indem Sie Ihren eigenen Wert für die verwenden`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-dnssec und EnableHostedZoneDNSSEC.

Console

So aktivieren Sie die DNSSEC-Signatur und erstellen eine KSK

1. Melden Sie sich bei der an AWS Management Console 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.

   Wenn Sie verwendet haben AWS CLI, können Sie die Vorgangs-ID aus der Ausgabe des `EnableHostedZoneDNSSEC()` Aufrufs verwenden, um get-change auszuführen oder GetChange 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 machen Sie dann die Schritte in rückgängigSchritt 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 Management Console 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.

   - Wenn es sich bei der übergeordneten Zone um eine über Route 53 verwaltete Domain handelt, gehen Sie wie folgt vor:

     Stellen Sie sicher, dass Sie den korrekten Signaturalgorithmus (ECDSAP256SHA256 und Typ 13) und den 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 Domäne aus, und klicken Sie dann neben DNSSEC, wählen Sie Verwalten von Schlüsseln aus.
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 die übergeordnete Zone auf Route 53 gehostet wird oder die Domain in einer anderen Registrierung verwaltet wird, wenden Sie sich an die übergeordnete Zone oder den Besitzer der Domainregistrierung, um diese Anweisungen zu befolgen:

  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.

  - 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 es abrufen, indem Sie in der Konsole auf View Information to create DS record (Informationen anzeigen, um einen DS-Datensatz zu erstellen) klicken und das Feld DS record (DS-Datensatz) kopieren, oder indem Sie die GetDNSSEC-API aufrufen und den Wert des Felds „DSRecord“ abrufen:

    ```
    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-Datensatz mithilfe von einzufügen AWS CLI, erstellt und benennt der Besitzer der übergeordneten Zone eine JSON-Datei ähnlich dem folgenden Beispiel. 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.

In Record name (Datensatzname) geben Sie den gleichen Namen ein wie der `$zone_name`, wählen Sie DS für den Record type (Datensatztyp) und geben Sie den Wert von `$ds_record_value` ins Feld Value (Wert) ein und wählen Sie Create records (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 im Route-53-DNS-Service befindet, kann der Besitzer der übergeordneten Zone die vollständige Verbreitung über die GetChange API 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 die 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 im Route-53-DNS-Service befindet, kann der Besitzer der übergeordneten Zone die vollständige Verbreitung über die GetChange API 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 DeactivateKeySigningKey APIs auf.

Beispielsweise:

```
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 Management Console 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 Management Console 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 Key-signing keys (KSKs) (Schlüsselsignierungschlüssel (KSKs) den KSK aus, den Sie deaktivieren möchten, und wählen Sie unter Actions (Aktionen) Edit KSK (KSK bearbeitenK), setzen Sie den KSK status (KSK-Status) auf Inactive (Inaktiv) und wählen Sie dann Save KSK (KSK speichern) aus.

Rollback: Rufen Sie ActivateKeySigningKey und EnableHostedZoneDNSSEC-APIs auf.

Beispielsweise:

```
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.

   Verwenden Sie die ID aus dem `EnableHostedZoneDNSSEC()` Aufruf, um GetChange sicherzustellen, 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 die Signatur nicht erneut aktivieren, können Sie die KSKs durch bereinigen DeleteKeySigningKey und 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 einen KSK zu erstellen, muss Route 53 einen vom Kunden verwalteten Schlüssel in 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 beim Erstellen eines asymmetrischen kundenverwalteten Schlüssels finden Sie unter Erstellen asymmetrischer kundenverwalteter Schlüssel im - AWS Key Management Service Entwicklerhandbuch. Informationen zum Auffinden der kryptografischen Konfiguration eines vorhandenen kundenverwalteten Schlüssels finden Sie unter Anzeigen der kryptografischen Konfiguration von kundenverwalteten Schlüsseln im - AWS Key Management Service Entwicklerhandbuch.
- 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 für Sie in erstellen AWS KMS , der mit DNSSEC-Signatur ohne zusätzliche AWS KMS Berechtigungen verwendet werden kann. 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 Schlüsselsignierungsschlüsseln (KSKs)

Wenn Sie DNSSEC-Signaturschlüssel aktivieren, erstellt Route 53 einen Schlüssel-Signaturschlüssel (KSK). Sie können pro gehostete Zone bis zu zwei KSKs in Route 53 nutzen. Nachdem Sie die DNSSEC-Signatur aktiviert haben, können Sie KSKs hinzufügen, entfernen oder bearbeiten.

Beachten Sie Folgendes, wenn Sie mit Ihren KSKs arbeiten:

- 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 dringend, einen CloudWatch Alarm einzurichten, der Sie benachrichtigt, wenn ein -`DNSSECInternalFailure` oder -`DNSSECKeySigningKeysNeedingAction`Fehler erkannt wird. Weitere Informationen finden Sie unter Überwachung von Hosting-Zonen mit Amazon CloudWatch.
- Mit den in diesem Abschnitt beschriebenen KSK-Vorgängen können Sie die KSKs Ihrer Zone rotieren. Weitere Informationen und ein step-by-step Beispiel finden Sie unter DNSSEC-Schlüsselrotation im Blogbeitrag Konfigurieren der DNSSEC-Signatur und -Validierung mit Amazon Route 53.

Um mit KSKs in der zu arbeiten AWS Management Console, folgen Sie den Anweisungen in den folgenden Abschnitten.

Hinzufügen eines Schlüsselsignaturschlüssels

Wenn Sie DNSSEC-Signatur aktivieren, erstellt Route 53 eine Schlüsselsignierung (KSK) für Sie. Sie können KSKs auch separat hinzufügen. Sie können pro gehosteter Zone bis zu zwei KSKs in Route 53 nutzen.

Wenn Sie eine KSK erstellen, müssen Sie Route 53 angeben oder anfordern, um einen vom Kunden verwalteten Schlüssel für die Verwendung mit dem KSK zu erstellen. Wenn Sie einen vom Kunden verwalteten, vom Kunden verwalteten Schlüssel bereitstellen oder erstellen, gelten 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 Management Console hinzuzufügen.

So fügen Sie eine KSK hinzu

1. Melden Sie sich bei der an AWS Management Console 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. Klicken Sie auf derDNSSECunterSchlüsselsignierungsschlüssel (KSKs), wählen SieZur erweiterten Ansicht wechseln, und klicken Sie dann unterAktionen, wählen SieKSK hinzufügenaus.
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, vom Kunden verwalteten Schlüssel ein, der für die DNSSEC-Signatur gilt, oder geben Sie einen Alias für einen neuen, vom Kunden verwalteten 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 Management Console zu editieren.

So bearbeiten Sie ein Tag

1. Melden Sie sich bei der an AWS Management Console 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. Klicken Sie auf der DNSSEC signing (DNSSEC-Signierung) unter Key-signing keys (KSKs) (Schlüsselsignierungsschlüssel (KSKs), wählen Sie Switch to advanced view (Zur erweiterten Ansicht wechseln), und dann unter Actions (Aktionen), wählen Sie Create KSK (KSK erstellen) 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 Management Console-Tabelle zu löschen.

So löschen Sie eine VPC

1. Melden Sie sich bei der an AWS Management Console 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. Klicken Sie auf derDNSSECunterSchlüsselsignierungsschlüssel (KSKs), wählen SieZur erweiterten Ansicht wechselnund dann unterAktionen, wählen SieKSK löschenaus.
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.

So verwendet Route 53 die Ihrem KSK AWS KMS zugeordnete

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 einen RRSIG, indem die `Sign` AWS KMS API für den zugeordneten KMS-Schlüssel aufgerufen wird. Weitere Informationen finden Sie unter Signieren im AWS KMS -API-Handbuch. Diese RRSIGs werden nicht auf das Limit für Ressourcendatensätze der Zone angerechet.

Ein RRSIG läuft ab. Um zu verhindern, dass die RRSIGs ablaufen, werden sie regelmäßig aktualisiert, indem sie alle ein bis sieben Tage regeneriert werden.

Die RRSIGs werden außerdem jedes Mal aktualisiert, wenn Sie eine dieser APIs aufrufen:

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Jedes Mal, wenn Route 53 eine Aktualisierung durchführt, generieren wir 15 RRSIGs, um die nächsten Tage abzudecken, falls auf den zugehörigen KMS-Schlüssel nicht 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`. Wir empfehlen dringend, diesen Zustand zu überwachen, indem Sie einen CloudWatch Alarm einrichten, wenn ein `DNSSECKeySigningKeysNeedingAction` Fehler erkannt wird, da die Validierung von Resolvern nach Ablauf des letzten RRSIG mit dem Fehlschlagen von Nachschlagevorgängen beginnt. 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 ECDSAP256SHA256.

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 wird die ZSK-Rotation aussetzen, wenn einer der KSK der Zone im `ACTION_NEEDED`-Status ist, da Route 53 die RRSIGs für DNSKEY-Ressourcendatensätze nicht regenerieren kann, um die Änderungen im ZSK der Zone zu berücksichtigen. 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 ein Datensatz mit dem Abfragenamen, aber nicht mit dem Abfragetyp übereinstimmt (z. B. die Abfrage nach web.example.com/AAAA, aber nur web.example.com/A ist vorhanden), geben wir einen minimalen NSEC-Datensatz (den nächsten sicheren) zurück, der alle unterstützten Ressourceneintragstypen 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-Signatur für Nicht-DNSKEY-Datensätze, um RRSIGs zu generieren, die für die Antwort spezifisch sind und 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 beheben, einschließlich der Aktivierung, Deaktivierung und mit Ihrer Schlüsselsignierungsschlüssel (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 einem -KeySigningKeyStatus) ändern, wenn Route 53 DNSSEC den Zugriff auf eine entsprechende verliert AWS KMS key (aufgrund einer Änderung der Berechtigungen oder des AWS KMS key Löschens).

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 den KSK repariert haben, aktivieren Sie ihn erneut mithilfe der Konsole oder der AWS CLI, wie unter beschriebenSchritt 2: Aktivieren der DNSSEC-Signatur und Erstellen einer KSK.

Um dieses Problem in Zukunft zu vermeiden, sollten Sie eine - Amazon CloudWatch Metrik hinzufügen, um den Status des KSK zu verfolgen, wie in vorgeschlagenKonfigurieren der DNSSEC-Signatur in Amazon Route 53.

KSK-Status lautetInternal failure (Interner Fehler)

Wenn ein KSK den Status Interner Fehler (oder `INTERNAL_FAILURE` KeySigningKey Status) hat, können Sie erst mit anderen DNSSEC-Entitäten zusammenarbeiten, wenn 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 den APIs zu beheben, versuchen Sie, die Signatur (EnableHostedZoneDNSSEC) zu aktivieren oder die Signatur (DisableHostedZoneDNSSEC) zu deaktivieren.

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.

Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr

Der Datenverkehr vereinfacht das Erstellen und Verwalten von Datensätzen 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 des Verkehrsflusses

Um die Nachverfolgung der Datensätze und ihrer Beziehungen zu erleichtern, vereinfacht der Traffic Flow die Erstellung von DNS-Einträgen mit den folgenden Funktionen:

Visual editor (Visueller Editor)

Mit dem visuellen Editor für Datenverkehrsfluss können Sie komplexe Datensätze 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. Mithilfe des Datenverkehrs können Sie alle diese Datensätze automatisch erstellen, indem Sie

einen Datensatz für eine Datenverkehrsrichtlinie 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**
>
> Mit dem Datenverkehrsfluss können Sie Datensätze nur in öffentlichen gehosteten Zonen erstellen.

Routing-Richtlinie auf Grundlage der geografischen Nähe

Wenn Sie den Verkehrsfluss verwenden, können Sie mithilfe der Geoproximitätskarte auf der visuellen Leinwand für den Verkehrsfluss intuitiver nachvollziehen, wie der Verkehr zu den einzelnen globalen Endpunkten geleitet wird. Weitere Informationen finden Sie unter Routing mit Geoproximität.

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.

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 Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.
2. Basierend auf dem Entwurf für Ihre Konfiguration erstellen Sie die Zustandsprüfungen, die Sie für Ihre Endpunkte verwenden möchten.
3. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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.
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

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 Verkehr an die folgenden AWS Ressourcen weiterleiten möchten, wählen Sie den entsprechenden Wert aus:

- CloudFront Verteilung — Wählen Sie A: IP-Adresse im IPv4-Format oder AAAA: IP-Adresse im IPv6-Format.
- ELB Application Load Balancer: Wählen Sie entweder A: IP-Adresse im IPv4-Format oder AAAA: IP-Adresse im IPv6-Format aus.
- ELB Classic Load Balancer: Wählen Sie entweder A: IP-Adresse im IPv4-Format oder AAAA: IP-Adresse im IPv6-Format aus.
- ELB Network Load Balancer: Wählen Sie entweder A: IP-Adresse im IPv4-Format oder AAAA: IP-Adresse im IPv6-Format aus.
- Elastic-Beanstalk-Umgebung: Wählen Sie A: IP-Adresse im IPv4-Format aus.
- Amazon-S3-Bucket konfiguriert als Website-Endpunkt: Wählen Sie A: IP address in IPv4 format.

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.

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.

Latenz-Regel

Wählen Sie diese Option, wenn Sie Ressourcen in mehreren Amazon-EC2-Rechenzentren haben, 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.

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 an eine 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 Amazon EC2 EC2-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 Routing mit Geoproximität.

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.

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.

Endpunkt

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 als DNS-Typ oder AAAA: IP-Adresse im IPv6-Format als DNS-Typ auswählen.

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 address in IPv4 format oder AAAA: IP address in IPv6 format für DNS type wählen.

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 address in IPv4 format oder AAAA: IP address in IPv6 format für DNS type wählen.

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 address in IPv4 format oder AAAA: IP address in IPv6 format für DNS type wählen.

Elastic Beanstalk-Umgebung

Wählen Sie diese Option aus, wenn Sie Datenverkehr an eine Elastic-Beanstalk-Umgebung weiterleiten möchten. Diese Option ist nur verfügbar, wenn Sie A: IP address in IPv4 format für DNS type wählen.

S3-Website-Endpunkt

Wählen Sie diese Option, wenn Sie Datenverkehr an einen Amazon-S3-Bucket leiten möchten, der als Website-Endpunkt konfiguriert ist. Diese Option ist nur verfügbar, wenn Sie A: IP address in IPv4 format für DNS type wählen.

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. Dies erfordert, dass Sie eine IP-Adresse im IPv4-Format in das Feld 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

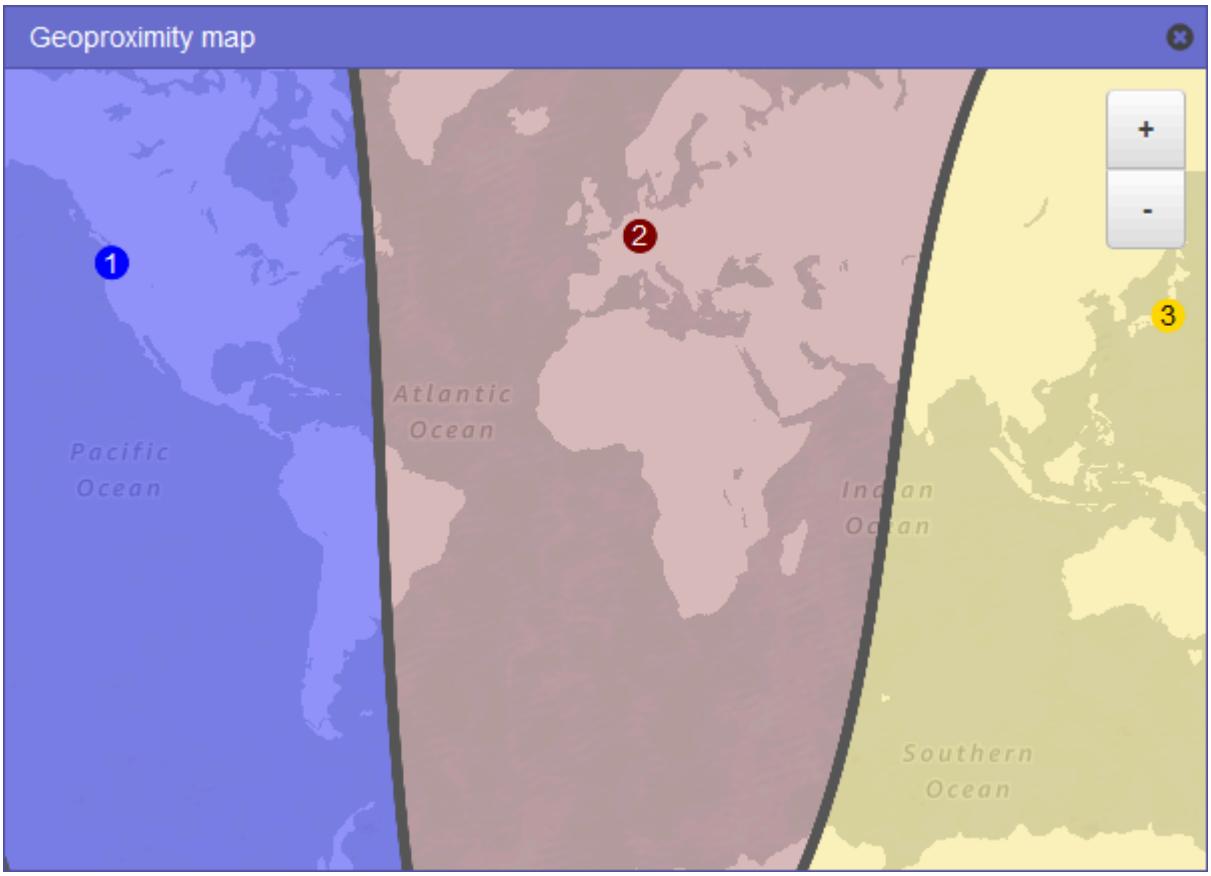
Geben Sie einen Wert ein, der dem Wert entspricht, den Sie für DNS type zu Beginn dieser Datenverkehrsrichtlinie eingegeben haben. Wenn Sie beispielsweise MX für DNS type (DNS-Typ) ausgewählt haben, geben Sie zwei Werte ein: die Priorität, die Sie einem E-Mail-Server zuweisen möchten, und den Domänennamen des E-Mail-Servers (beispielsweise `10 sydney.mail.example.com`).

Weitere Informationen zu unterstützten DNS-Typen finden Sie unter Unterstützte DNS-Datensatztypen.

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 Routing mit Geoproximität.

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 MyTrafficPolicy erstellen, 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.

So erstellen Sie eine andere Version einer Datenverkehrsrichtlinie

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 Datenverkehrsrichtlinie durch Importieren 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 AWS CLI - Befehlsreferenz.

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.

So erstellen Sie eine Datenverkehrsrichtlinie durch Importieren eines JSON-Dokuments

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

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.

So zeigen Sie Datenverkehrsrichtlinien-Versionen und die zugehörigen Richtliniendatensätze an

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console 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:

So löschen Sie Datenverkehrsrichtlinien-Versionen und Datenverkehrsrichtlinien

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console 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 an, in der Sie den Richtliniendatensatz erstellen möchten, und den Namen der Domäne oder Subdomäne, für den 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

- Aktualisieren von Richtliniendatensätzen
- Löschen von Richtliniendatensätzen

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.

So erstellen Sie einen Richtliniendatensatz

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console 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

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 des Richtliniendatensatzes

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 Domänennamen oder den Subdomänennamen in der angegebenen gehosteten Zone zu verwenden, klicken Sie auf Add another policy record, und geben Sie den entsprechenden Domänennamen oder Subdomänennamen und den TTL-Wert 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.

So aktualisieren Sie einen Richtliniendatensatz

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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“.

So löschen Sie einen Richtliniendatensatz

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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? Amazon Route 53 Resolver

Amazon Route 53 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 VPCs verfügbar.

> **Note**
>
> Amazon Route 53 Resolver hieß früher Amazon DNS-Server, wurde aber umbenannt, als Resolver-Regeln sowie eingehende und ausgehende Endpunkte eingeführt wurden. Weitere Informationen finden Sie unter Amazon-DNS-Server im Benutzerhandbuch von Amazon Virtual Private Cloud.

Eine Amazon VPC stellt eine Verbindung zu einem Route 53 Resolver an einer VPC+2-IP-Adresse her. Diese VPC+2-Adresse stellt eine Verbindung zu einem Route 53 Resolver innerhalb einer Availability Zone her.

Ein Route 53 Resolver beantwortet automatisch DNS-Abfragen für:

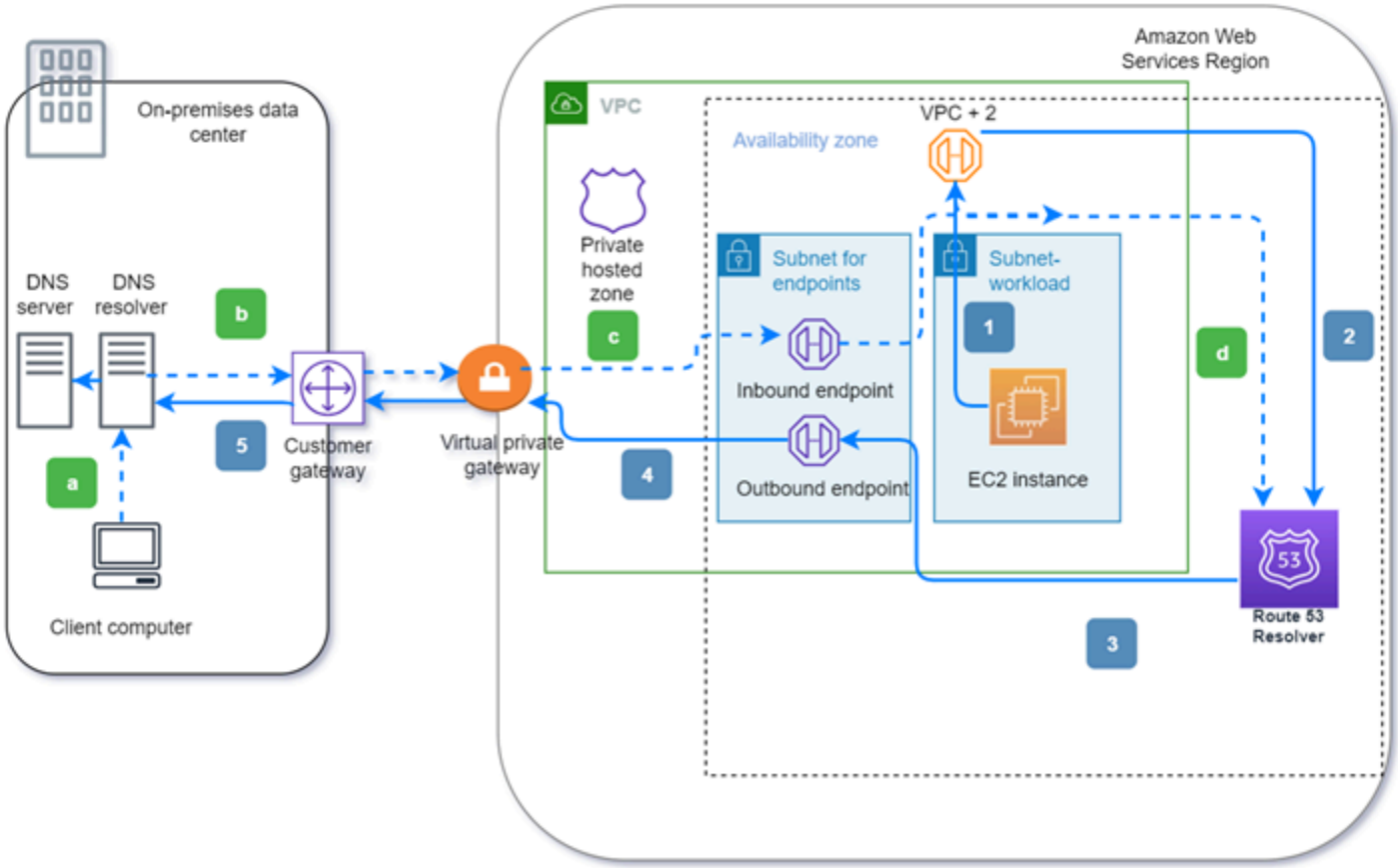
- Lokale VPC-Domainnamen für EC2-Instances (zum Beispiel ec2-192-0-2-44.compute-1.amazonaws.com).
- Datensätze in privaten gehosteten Zonen (z. B. acme.example.com).
- Für alle anderen Domainnamen führt Route 53 rekursive Suchen anhand öffentlicher Namensserver im Internet durch.

Wenn Sie Workloads haben, die sowohl VPCs als auch On-Premises-Ressourcen nutzen, müssen Sie auch DNS-Einträge auflösen, die On-Premises gehostet werden. In ähnlicher Weise müssen diese lokalen Ressourcen möglicherweise Namen auflösen, die auf gehostet werden. AWS Mithilfe von Resolver-Endpunkten und Regeln für die bedingte Weiterleitung können Sie DNS-Abfragen zwischen Ihren On-Premises-Ressourcen und VPCs auflösen, um ein Hybrid-Cloud-Setup über VPN oder Direct Connect (DX) zu 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 Amazon–EC2-Instance muss eine DNS-Abfrage 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 mit Route 53 Resolver herstellt.

2. Eine Route-53-Resolver-Weiterleitungsregel ist für die Weiterleitung von Abfragen an internal.example.com im On-Premises-Rechenzentrum konfiguriert.
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 AWS Direct Connect oder sein AWS Site-to-Site VPN, dargestellt als virtuelles privates Gateway.
5. Der On-Premises-DNS-Resolver löst die DNS-Abfrage für internal.example.com auf und gibt die Antwort über denselben Pfad in umgekehrter Reihenfolge an die Amazon-EC2-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. AWS Direct Connect oder AWS Site-to-Site VPN, die als virtuelles Gateway dargestellt wird.
d. Der eingehende Endpunkt sendet die Anfrage an den Route 53 Resolver, und Route 53 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 VPCs und Ihrem Netzwerk

Der Resolver enthält Endpunkte, die Sie konfigurieren, um DNS-Abfragen an und von Ihrer On-Premises-Umgebung zu beantworten.

> **Note**
>
> Das Weiterleiten privater DNS-Abfragen an eine beliebige VPC CIDR+2-Adresse von Ihren On-Premises-DNS-Servern wird nicht unterstützt und kann zu instabilen Ergebnissen führen. Stattdessen empfehlen wir Ihnen, einen eingehenden Resolver-Endpunkt zu verwenden.

Sie können auch die DNS-Auflösung zwischen Resolver und DNS-Auflösungen 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 NAT-Gateway (Network AWS Direct Connect Address Translation) verbunden ist

Bevor Sie mit der Weiterleitung von Abfragen beginnen, erstellen Sie eingehende und/oder ausgehende Endpunkte in der verbundenen VPC. Diese Endpunkte bieten einen Pfad für eingehende oder ausgehende Abfragen:

Eingehender Endpunkt: DNS-Resolver in Ihrem Netzwerk können DNS-Abfragen über diesen Endpunkt an Route 53 weiterleiten

Auf diese Weise können Ihre DNS-Resolver problemlos Domainnamen für AWS Ressourcen wie EC2-Instances oder Datensätze in einer privat gehosteten Route 53-Zone auflösen. Weitere Informationen finden Sie unter So leiten DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Route 53 Resolver Endpunkte weiter.

Ausgehender Endpunkt: Resolver leitet Abfragen 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 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. Weitere Informationen finden Sie unter So leiten Route 53-Resolver DNS-Abfragen von Ihren VPCs an Ihr Netzwerk weiter.

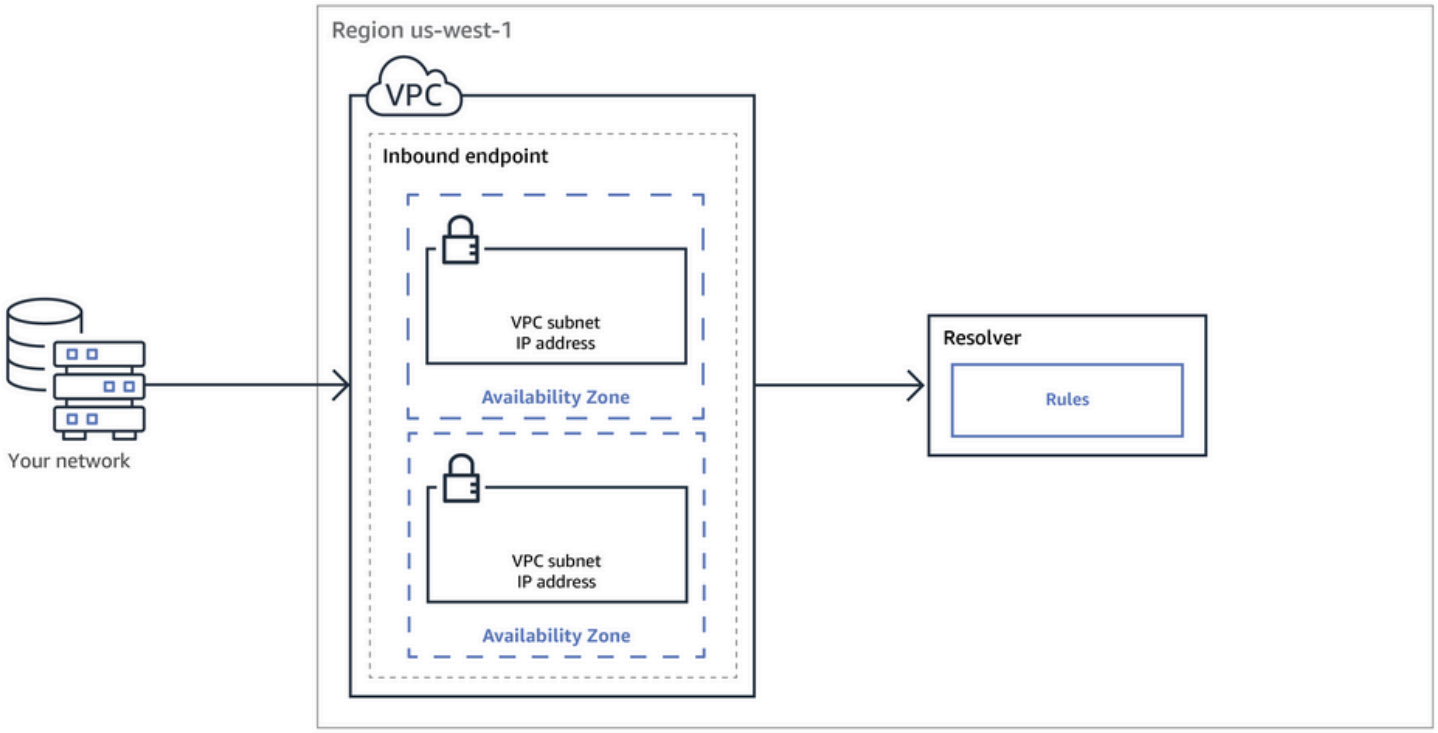
Wie Amazon VPC ist Resolver regional. In jeder Region, in der Sie über VPCs verfügen, können Sie wählen, ob Sie Abfragen von Ihren VPCs an Ihr Netzwerk (ausgehende Abfragen) oder von Ihrem Netzwerk an Ihre VPCs (eingehende Abfragen) weiterleiten möchten oder beides.

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.

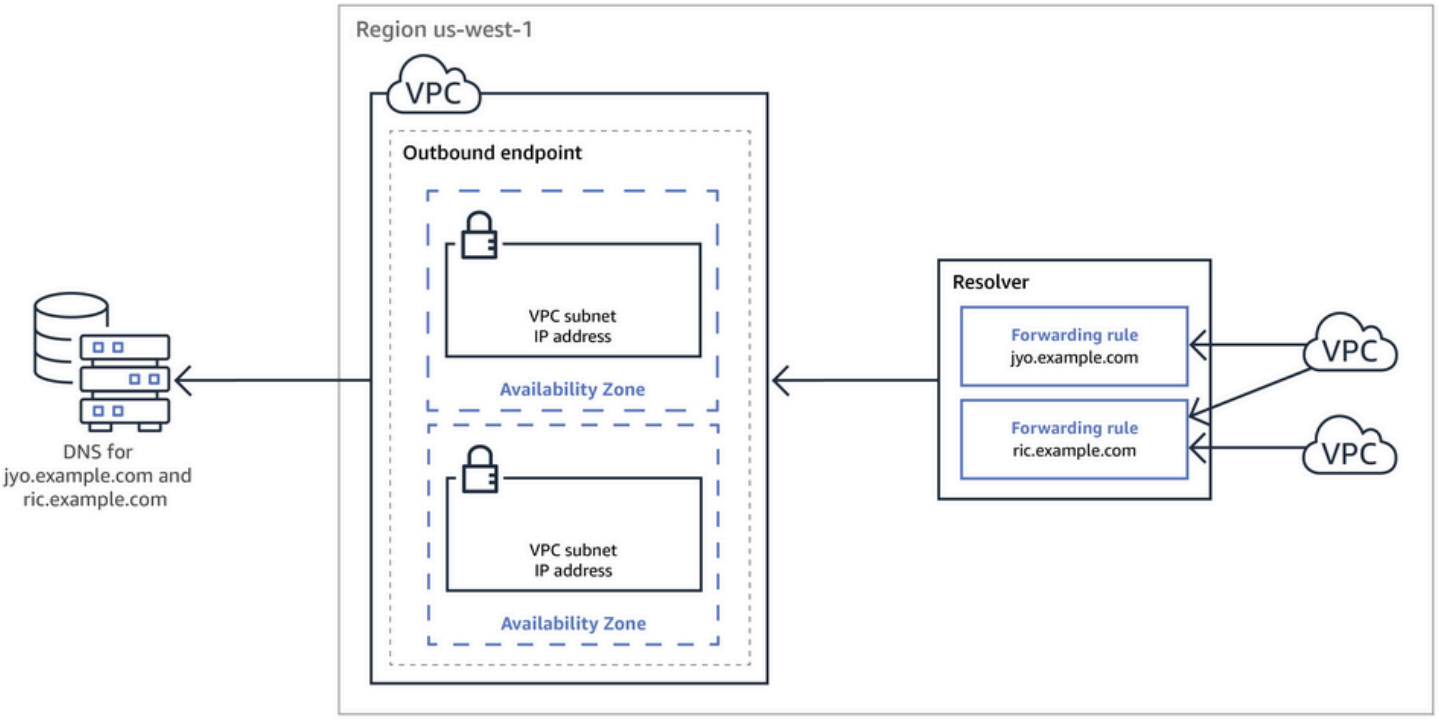
> **Note**
>
> Wenn Sie einen Resolver-Endpunkt erstellen, können Sie keine VPC angeben, für die das Instance-Tenancy-Attribut auf `dedicated` festgelegt ist. Weitere Informationen finden Sie unter .

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 an, über die Sie eingehende DNS-Abfragen weiterleiten möchten, oder die IP-Adressen, von denen ausgehende Abfragen stammen sollen. Für jede IP-Adresse, die Sie angeben, erstellt Resolver automatisch eine VPC Elastic Network-Schnittstelle.

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-Instance in einer Ihrer VPCs zu einem DNS-Resolver in Ihrem Netzwerk an.



Eine Übersicht über VPC Netzwerkschnittstellen finden Sie unterElastic Network-Schnittstelleim Amazon VPC User Guideaus.

Topics

So leiten DNS-Resolver in Ihrem Netzwerk DNS-Abfragen an Route 53 Resolver Endpunkte weiter

Wenn Sie DNS-Abfragen von Ihrem Netzwerk an Route 53 in einer AWS -Region weiterleiten möchten, führen Sie die folgenden Schritte aus:

1. Sie erstelle einen Route 53 eingehenden Endpunkt in einer VPC und geben die IP-Adressen an, an die die Resolver in Ihrem Netzwerk DNS-Abfragen weiterleiten.

   Für jede IP-Adresse, die Sie für den eingehenden Endpunkt angeben, erstellt Resolver eine VPC Elastic Network-Schnittstelle 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 Resolver DNS-Abfragen auf, die ihren Ursprung in Ihrem Netzwerk haben:

1. Ein Webbrowser oder eine andere Anwendung in Ihrem Netzwerk sendet eine DNS-Abfrage für einen Domainnamen, den Sie an 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 Resolver weiter.
4. Resolver ruft den entsprechenden Wert für den Domainnamen in der DNS-Abfrage ab, entweder intern oder über eine rekursive Suche anhand öffentlicher Namenserver.
5. Der 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. Mit dem von Resolver zurückgegebenen Wert sendet die Anwendung eine HTTP-Anfrage, beispielsweise für ein Objekt in einem Amazon S3-Bucket.

Das Erstellen eines Eingangsendpunkts ändert nichts am Verhalten von Resolver, sondern stellt lediglich einen Pfad von einem Standort außerhalb des AWS Netzwerks zum Resolver bereit.

So leiten Route 53-Resolver DNS-Abfragen von Ihren VPCs an Ihr Netzwerk weiter

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 Route 53–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.
   - Die IP-Adressen in Ihrer VPC, von denen Resolver DNS-Abfragen weiterleiten soll. Für Hosts in Ihrem Netzwerk sind dies die IP-Adressen, von denen die DNS-Abfragen stammen.
   - Eine VPC-Sicherheitsgruppe

   Für jede IP-Adresse, die Sie für den ausgehenden Endpunkt angeben, erstellt Amazon VPC eine Elastic Network-Schnittstelle in der VPC, die Sie angeben. Weitere Informationen finden Sie unter Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten.
2. Sie erstellen eine oder mehrere Regeln, um die Domainnamen der DNS-Abfragen anzugeben, die an Resolver in Ihrem Netzwerk weiterleiten soll. Sie legen auch die IP-Adressen der Resolver fest. Weitere Informationen finden Sie unter Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden.
3. Sie verknüpfen alle Regeln mit den VPCs, für die Sie DNS-Abfragen an Ihr Netzwerk weiterleiten möchten.

Themen

- Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden
- So bestimmt Resolver, ob der Domainname in einer Abfrage einer Regel entspricht
- So bestimmt Resolver, wohin DNS-Abfragen weitergeleitet werden sollen
- Verwenden von Regeln in mehreren Regionen

- Domainnamen, für die Resolver automatisch definierte Systemregeln erstellt

Verwenden von Regeln zum Steuern, welche Abfragen an Ihr Netzwerk weitergeleitet werden

Mithilfe von Regeln wird gesteuert, welche Route 53 Resolver DNS-Abfragen an DNS-Resolver in Ihrem Netzwerk weiterleitet und welche Abfragen Resolver selbst beantwortet.

Es gibt mehrere Möglichkeiten zum Kategorisieren von Regeln. Eine Möglichkeit ist die Kategorisierung nach Ersteller der Regeln:

- Automatisch definierte Regeln – Resolver erstellt automatisch definierte Regeln und verknüpft diese mit Ihren VPCs. Die meisten dieser Regeln gelten für die AWS-spezifischen Domainnamen, für die Resolver Anfragen beantwortet. Weitere Informationen finden Sie unter Domainnamen, für die Resolver automatisch definierte Systemregeln erstellt.
- Benutzerdefinierte Regeln - Sie erstellen benutzerdefinierte Regeln und verknüpfen diese mit VPCs. Derzeit können Sie nur eine Art von benutzerdefinierten Regeln erstellen, nämlich bedingte Weiterleitungsregeln (auch einfach als Weiterleitungsregeln bezeichnet). Weiterleitungsregeln bewirken, dass Resolver DNS-Abfragen von Ihren VPCs an die IP-Adressen für DNS-Resolver in Ihrem Netzwerk weiterleitet.

  Wenn Sie eine Weiterleitungsregel für dieselbe Domain als automatisch definierte Regel erstellen, leitet Resolver Abfragen für diesen Domainname an DNS-Resolver in Ihrem Netzwerk basierend auf den Einstellungen in der Weiterleitungsregel weiter.

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 Resolver das in einer Weiterleitungsregel definierte Verhalten selektiv überschreibt. Wenn Sie eine Systemregel erstellen, löst Resolver DNS-Abfragen für bestimmte Subdomains auf, die andernfalls von DNS-Resolvern in Ihrem Netzwerk aufgelöst werden.

  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 - erstellt automatisch eine rekursive Regel mit dem Namen Internet Resolver. Diese Regel führt dazu, dass Route 53 als rekursiver Resolver für alle Domainnamen arbeitet, für die Sie keine benutzerdefinierten Regeln erstellt haben, und für die 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 AWS Domainnamen), für öffentliche AWS Domainnamen oder für alle 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. Darüber hinaus geben Sie die IP-Adressen der DNS-Resolver in Ihrem Netzwerk an, an die Sie die Abfragen weiterleiten möchten. Anschließend verknüpfen Sie alle Regeln mit den 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 in beliebiger Kombination den VPCs in 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 Abfragen für amazonaws.com an Ihr Netzwerk weiterleiten möchten, erstellen Sie eine Regel, geben Sie für den Domainnamen amazonaws.com und für den Regeltyp Forward (Weiterleiten) an.

> **Note**
>
> Resolver leitet DNS-Abfragen für einige Subdomains von amazonaws.com nicht automatisch weiter, selbst dann nicht, wenn Sie eine Weiterleitungsregel für amazonaws.com erstellen. Weitere Informationen finden Sie unter Domainnamen, für die 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 Abfragen an Ihr Netzwerk weiterleiten möchten, erstellen Sie eine Regel. Geben Sie für den Domainnamen "." (Punkt) an und verknüpfen Sie die Regel mit den VPCs, für die alle DNS-Abfragen an Ihr Netzwerk weitergeleitet werden sollen. Der Resolver leitet immer noch nicht alle DNS-Anfragen an Ihr Netzwerk weiter, da die Verwendung eines DNS-Resolvers außerhalb von einige Funktionen beeinträchtigen würde. AWS 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 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 im 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 Resolver automatisch definierte Systemregeln erstelltaufgeführt sind.

> **Important**
>
> Wenn Sie alle Domainnamen an Ihr Netzwerk weiterleiten, einschließlich der Domainnamen, die Resolver bei der Erstellung einer "."-Regel ausschließt, funktionieren einige Funktionen möglicherweise nicht mehr.

So bestimmt Resolver, ob der Domainname in einer Abfrage einer Regel entspricht

Route 53 vergleicht den Domainnamen in der DNS-Abfrage mit dem Domainnamen in den Regeln, die mit der VPC verknüpft sind, aus der die Abfrage stammt. 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 Resolver die folgenden Domainnamen in einer DNS-Abfrage als Übereinstimmung:

- 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 in mehr als einer Regel mit dem Domainnamen übereinstimmt (wie beispielsweise example.com und www.example.com), leitet Resolver ausgehende DNS-Abfragen entsprechend der Regel weiter, die den spezifischsten Domainnamen (www.example.com) enthält.

So bestimmt Resolver, wohin DNS-Abfragen weitergeleitet werden sollen

Wenn eine Anwendung, die auf einer EC2 Instance in einer VPC ausgeführt wird, eine DNS-Abfrage sendet, führt Route 53 Resolver die folgenden Schritte aus:

1. Resolver führt Prüfungen auf Domainnamen in Regeln aus.

   Wenn der Domainname in einer Abfrage mit dem Domainnamen in einer Regel übereinstimmt, leitet Resolver die Abfrage an die IP-Adresse weiter, die Sie beim Erstellen 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.

   Weitere Informationen finden Sie unter So bestimmt Resolver, ob der Domainname in einer Abfrage einer Regel entspricht.
2. Resolver Endpunkt leitet DNS-Abfragen basierend auf den Einstellungen in der "."-Regel weiter.

   Wenn der Domainname in einer Abfrage nicht dem Domainnamen in einer anderen Regel übereinstimmt, leitet Resolver die Anfrage basierend auf den Einstellungen in der automatisch

definierten "."-Regel (Punkt-Regel) weiter. Die Punktregel gilt für alle Domainnamen mit Ausnahme einiger AWS interner Domainnamen und Datensatznamen in privaten Hosting-Zonen. Diese Regel bewirkt, dass Resolver DNS-Abfragen an öffentliche Nameserver weiterleitet, wenn die Domainnamen in 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. Resolver gibt die Antwort an die Anwendung zurück, die die Abfrage übermittelt hat.

Verwenden von Regeln in mehreren Regionen

Route 53 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 Resolver automatisch definierte Systemregeln erstellt

Der Resolver erstellt automatisch definierte Systemregeln, die definieren, wie Abfragen für ausgewählte Domains standardmäßig aufgelöst werden:

- Für private gehostete Zonen und für Amazon EC2 spezifische Domainnamen (z. B. compute.amazonaws.com und compute.internal) stellen automatisch definierte Regeln sicher, dass Ihre privat gehosteten Zonen und EC2-Instances weiterhin aufgelöst werden, wenn Sie bedingte Weiterleitungsregeln für weniger spezifische Domainnamen wie "." (Punkt) oder "com" erstellen.
- 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 bewirken, dass Resolver DNS-Abfragen für bestimmte Domains und Subdomains lokal auflöst.) Eine solche erstellte Systemregel verbessert die Leistung, reduziert die Anzahl der Abfragen, die an Ihr Netzwerk weitergeleitet werden, und senkt die 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 im Resolver.

Resolver erstellt die folgenden automatisch definierten Regeln.

Regeln für privat gehostete Zonen

Für jede privat gehostete Zone, die Sie mit einer VPC verknüpfen, erstellt Resolver eine Regel und verknüpft diese mit der VPC. Wenn Sie die privat gehostete Zone mit mehreren VPCs verknüpfen, verknüpft Resolver die Regel mit denselben 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. Resolver leitet DNS-Abfragen für diese Domainnamen an die autoritativen Nameserver für die VPC weiter.

> **Note**
>
> Resolver erstellt die meisten dieser Regeln, wenn Sie die `enableDnsHostnames`-Flag für eine VPC`true` festlegen. Resolver erstellt die Regeln, auch wenn Sie keine Resolver-Endpunkte verwenden.

Resolver erstellt die folgenden automatisch definierten Regeln und verknüpft sie mit einer VPC, wenn Sie für das Flag `enableDnsHostnames` für die VPC `true` festlegen:

- *Region-name*.compute.internal, z. B. eu-west-1.compute.internal. Die Region us-east-1 verwendet diesen Domainnamen nicht.
- *Region-name*.compute.*amazon-domain-name*, z. B. 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 Domainnamen.

Die folgenden automatisch definierten Regeln gelten für die Reverse-DNS-Suche für die Regeln, die Resolver erstellt, wenn Sie das Flag `enableDnsHostnames` für die VPC auf `true` festlegen.

- 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 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

Resolver erstellt die folgenden automatisch definierten Regeln und verknüpft sie mit Ihrer VPC, wenn Sie die VPC über Transit Gateway oder VPC Peering verbinden und DNS-Unterstützung aktivieren:

- Die Reverse-DNS-Suche für die IP-Adressbereiche der Peer-VPC, z. B. 0.192.in-addr.arpa

Wenn Sie einen IPv4-CIDR-Block zu einer VPC hinzufügen, fügt 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*.compute.*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

Resolver erstellt eine "."-Regel (Punkt-Regel), die für alle Domainnamen gilt, die nicht zuvor in diesem Thema angegeben wurden. Die "."-Regel verfügt über einen Typ von Recursive (Rekursiv). Dies bedeutet, dass Resolver durch diese Regel als rekursiver Resolver wirkt.

Erwägungen beim Erstellen von ein- und ausgehenden Endpunkten

Bevor Sie Resolver-Endpunkte 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 den VPCs, in denen Sie Endpunkte erstellen
- Wenn Sie Regeln freigeben, geben Sie auch ausgehende Endpunkte frei
- Auswählen von Protokollen für die Endpunkte
- Verwenden von Resolvern in für Dedicated-Instance-Tenancy konfigurierten VPCs

Anzahl der eingehenden und ausgehenden Endpunkte in den einzelnen -Regionen

Wenn Sie DNS für die VPCs in einer AWS Region mit DNS für Ihr Netzwerk integrieren möchten, benötigen Sie in der Regel einen Resolver-Endpunkt für eingehende Anfragen (für DNS-Abfragen, die Sie an Ihre VPCs weiterleiten) und einen ausgehenden Endpunkt (für Anfragen, die Sie von Ihren VPCs an Ihr Netzwerk weiterleiten). 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 bei Route 53 Resolver.) Wenn Resolver mehr Abfragen verarbeiten muss, können Sie weitere IP-Adressen zu Ihrem vorhandenen Endpunkt hinzufügen, anstatt einen neuen Endpunkt hinzufügen zu müssen.
- Resolver-Preise 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 Resolver-Preisen 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 Endpunkte 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 Resolver eingehende DNS-Abfragen mittels Datensätzen in einer privat gehosteten Zone auflöst, setzen Sie die privat gehostete Zone mit der VPC in Bezug, in der Sie den eingehenden Endpunkt erstellt haben. Weitere Informationen zum Zuordnen von privat gehosteten Zonen mit VPCs finden Sie unter 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 VPCs gepeert wird. 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 freigegebenen Subnetzen finden Sie unterArbeiten mit freigegebenen VPCs im Amazon VPC User Guideaus.

Verbindung zwischen Ihrem Netzwerk und den VPCs, in denen Sie Endpunkte erstellen

Sie müssen über eine der folgenden Verbindungen zwischen Ihrem Netzwerk und den VPCs verfügen, in denen Sie Endpunkte erstellen:

- Eingehende Endpunkte - Sie müssen entweder eine AWS 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 AWS 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, von dem Sie möchten, dass Resolver ihn zum Weiterleiten von DNS-Abfragen an Ihr Netzwerk verwendet. 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 mehr als ein AWS Konto verwendet haben, um VPCs in einer AWS Region zu erstellen, 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 haben.

Auf diese Weise können Sie einen ausgehenden Endpunkt in einer Region verwenden, um DNS-Anfragen von mehreren VPCs an Ihr Netzwerk weiterzuleiten, auch wenn die VPCs mit unterschiedlichen Konten erstellt wurden. AWS

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 mit Hilfe des Route-53-Resolver 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.
- 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.

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.

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 Resolvern in für Dedicated-Instance-Tenancy konfigurierten VPCs

Wenn Sie einen Resolver-Endpunkt erstellen, können Sie keine VPC angeben, für die das Instance-Tenancy-Attribut auf `dedicated` festgelegt ist. Resolver wird nicht auf Einzelmandantenhardware ausgeführt.

Sie können Resolver weiterhin verwenden, um DNS-Abfragen aufzulösen, die aus einer VPC stammen. 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.

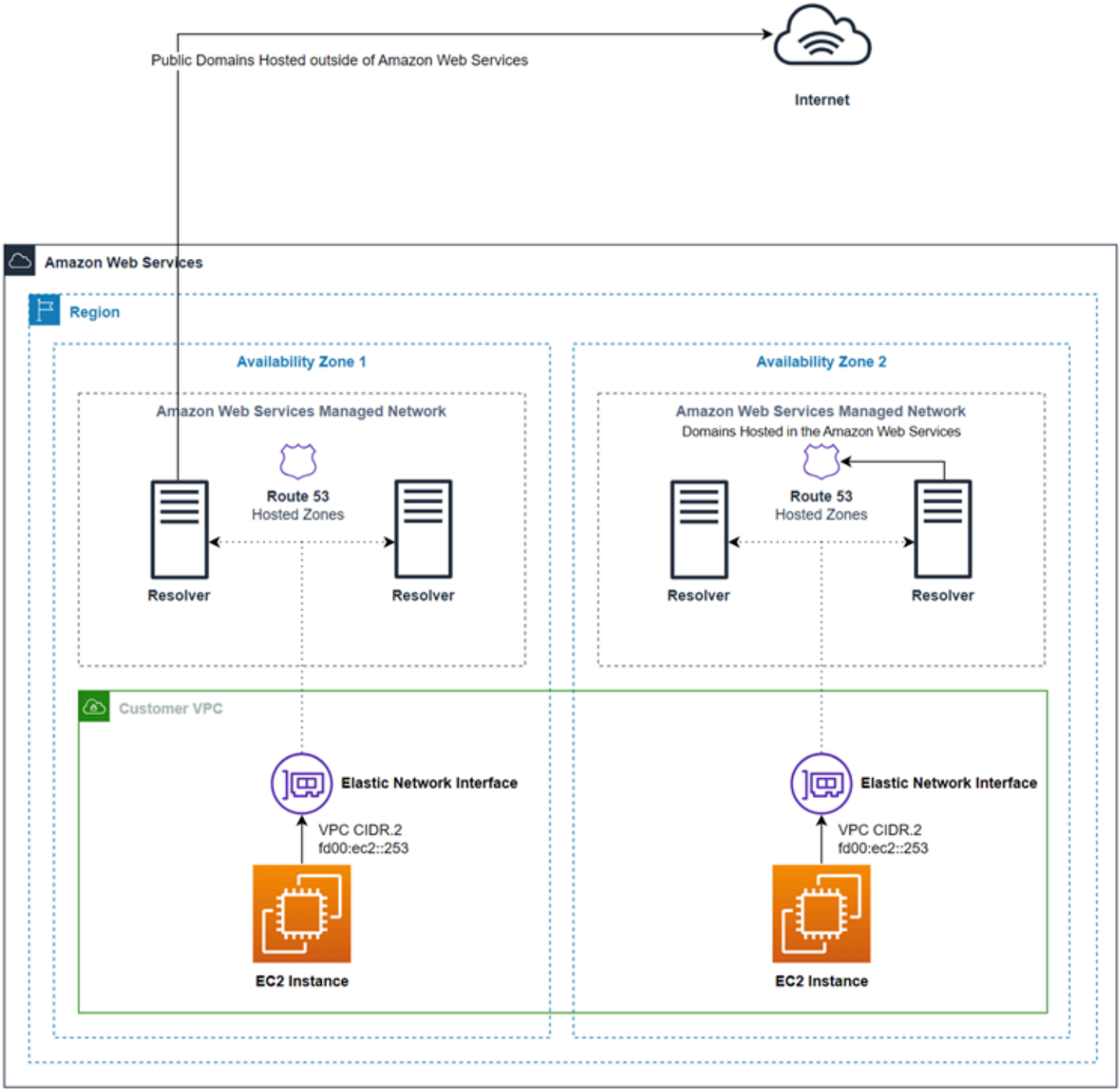
Verfügbarkeit und Skalierung von Route 53 Resolver

Amazon Route 53 Resolver, läuft auf der Amazon VPC CIDR + 2-Adresse und fd00:ec2: :253, ist standardmäßig in allen VPCs verfügbar und reagiert rekursiv auf DNS-Abfragen für öffentliche Aufzeichnungen, Amazon VPC-spezifische DNS-Namen und Route 53-private gehostete Zonen. Der Route 53 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 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 den Time-To-Live-Wert (TTL) hinausgeht, um die 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 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 Amazon EC2 EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch. Diese Metrik kann vom Agenten auch an CloudWatch Metriken gemeldet werden. CloudWatch Da der Route 53 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 Resolver innerhalb der Grenzen einer VPC skalieren kann, was von Natur aus 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 Resolver DNS-Abfragen innerhalb von Availability Zones auflöst.



Erste Schritte mit Route 53 Resolver

Die Route 53 Resolver-Konsole enthält einen Assistenten, der Sie durch die folgenden Schritte für die ersten Schritte mit 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 Resolver mit dem Assistenten

1. Melden Sie sich bei der Resolver-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53resolver/.
2. Wählen Sie auf der Seite Welcome to Route 53 Resolver (Willkommen zu Route 53 Resolver) die Option Configure endpoints (Endpunkte erstellen).
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:

   - Inbound and outbound (Eingehend und ausgehend): Der Assistent führt Sie durch die Einstellungen, mit denen Sie sowohl DNS-Abfragen von Resolvern in Ihrem Netzwerk zu Resolver in einer VPC als auch bestimmte Abfragen (z. B. example.com oder example.net) von einer VPC an Resolver in Ihrem Netzwerk weiterleiten können.
   - Inbound only (Nur eingehend): Der Assistent führt Sie durch die Einstellungen, mit denen Sie DNS-Abfragen von Resolvern in Ihrem Netzwerk zu 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-Abfragen an Ihre VPCs

Zum Weiterleiten von DNS-Abfragen von Ihrem Netzwerk an Resolver 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 AWS Direct Connect Verbindung oder eine VPN-Verbindung mit Ihrem Netzwerk verbinden.

Themen

- Konfigurieren von Weiterleitungen eingehender Abfragen

- Werte, die Sie beim Erstellen oder Bearbeiten von eingehenden Endpunkten angeben

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.
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:

Outpost-ID

Wenn Sie den Endpunkt für einen Resolver auf einer AWS Outposts VPC erstellen, ist dies die AWS Outposts ID.

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 ausgehenden DNS-Abfragen von Ihrem Netzwerk durchlaufen diese VPC auf dem Weg zu 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. Sie können diesen Wert nicht ändern, nachdem Sie einen 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

Beim Endpunkttyp kann es sich um IPv4-, um IPv6- oder um Dual-Stack-IP-Adressen handeln. Bei einem Dual-Stack-Endpunkt hat der Endpunkt sowohl eine IPv4- als auch eine IPv6-Adresse, an die Ihr DNS-Resolver in Ihrem Netzwerk eine DNS-Abfrage weiterleiten kann.

> **Note**
>
> Aus Sicherheitsgründen verweigern wir allen Dual-Stack- und IPv6-IP-Adressen den direkten IPv6-Verkehr aus dem öffentlichen Internet.

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. 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 festlegen, erstellt Resolver eine Amazon VPC Elastic Network-Schnittstelle. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente bei Route 53 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 ENIs zuweisen möchten. 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 in Ihrem Netzwerk, an die DNS-Abfragen weitergeleitet werden sollen.

Wählen Sie, ob Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst festlegen möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie entweder eine IPv4- oder eine IPv6-Adresse 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 über den Route-53-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.
- 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.

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

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.

Weiterleiten von ausgehenden DNS-Abfragen an Ihr Netzwerk

Zum Weiterleiten von DNS-Abfragen, die von Amazon EC2-Instances in einer oder mehreren VPCs in Ihrem Netzwerk stammen, erstellen Sie einen ausgehenden Endpunkt und eine oder mehrere Regeln.

Ausgehender Endpunkt

Um DNS-Abfragen von Ihren 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 AWS Direct Connect VPC-Verbindung oder ein NAT-Gateway (Network Address Translation) mit Ihrem Netzwerk verbinden müssen. Beachten Sie, dass Sie den gleichen ausgehenden Endpunkt für mehrere VPCs in derselben Region verwenden oder mehrere ausgehende Endpunkte erstellen können. Wenn Sie möchten, dass Ihr ausgehender Endpunkt DNS64 verwendet, können Sie DNS64 mit Amazon Virtual Private Cloud aktivieren. Weitere Informationen finden Sie unter DNS64 und NAT64 im Amazon VPC Benutzerhandbuch.

Die Ziel-IP aus der Route 53-Resolver-Regel wird vom 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 Resolver erneut, eine zufällige IP-Adresse unter den Ziel-IPs auszuwählen.

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 Regel gibt einen Domainnamen an. Anschließend verknüpfen Sie Regeln mit den VPCs, für die Sie Abfragen an Ihr Netzwerk weiterleiten möchten.

Weitere Informationen finden Sie unter den folgenden Themen:

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

Konfigurieren von Weiterleitungen ausgehender Abfragen

Um Resolver so zu konfigurieren, dass aus Ihrer VPC stammende DNS-Abfragen an Ihr Netzwerk weitergeleitet werden, führen Sie die folgenden Schritte aus.

> **Important**
>
> Nachdem Sie einen ausgehenden Endpunkt erstellt haben, müssen Sie eine oder mehrere Regeln erstellen und diese mit mindestens einer VPC verknüpfen. 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

> **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.

So erstellen Sie Weiterleitungsregeln und verknüpfen diese mit einer oder mehreren VPCs

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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:

Outpost-ID

Wenn Sie den Endpunkt für einen Resolver auf einer AWS Outposts VPC erstellen, ist dies die AWS Outposts ID.

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

Beim Endpunkttyp kann es sich um IPv4-, um IPv6- oder um Dual-Stack-IP-Adressen handeln. Bei einem Dual-Stack-Endpunkt hat der Endpunkt sowohl eine IPv4- als auch eine IPv6-Adresse, an die Ihr DNS-Resolver in Ihrem Netzwerk eine DNS-Abfrage weiterleiten kann.

> **Note**
>
> Aus Sicherheitsgründen verweigern wir allen Dual-Stack- und IPv6-IP-Adressen den direkten IPv6-Verkehr auf das öffentliche Internet.

IP-Adressen

Die IP-Adressen in Ihrer VPC, an die 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 Resolver-IP-Adressen an, wenn Sie die Regeln erstellen, die Sie mit einer oder mehreren VPCs verknüpfen. 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 festlegen, erstellt Resolver eine Amazon VPC Elastic Network-Schnittstelle. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente bei Route 53 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. Beim Weiterleiten von DNS-Abfragen wählt Resolver IP-Adressen nicht auf Grundlage 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, ob Resolver aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst festlegen möchten.

Wenn Sie die IP-Adresse selbst angeben möchten, geben Sie eine IPv4- oder IPv6-Adresse oder beides 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 über den Route-53-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.

Derzeit wird die TLS-SNI-Erweiterung für die DoH-Abfragen über den ausgehenden Endpunkt nicht unterstützt.

Tags

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.

Regeltyp

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.
- System – Wählen Sie diese Option, wenn Sie möchten, dass Resolver das Verhalten selektiv überschreibt, das in einer Weiterleitungsregel definiert ist. Wenn Sie eine Systemregel erstellen, löst Resolver DNS-Abfragen für bestimmte Subdomains auf, die andernfalls von DNS-Resolvern in Ihrem Netzwerk aufgelöst werden.

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.

VPCs, die diese Regel verwenden

Die VPCs, die diese Regel verwenden, um DNS-Abfragen für den oder die angegebenen Domainnamen weiterzuleiten. Sie können eine Regel auf beliebig viele VPCs anwenden.

Domainname

DNS-Abfragen für diesen Domainnamen werden an die IP-Adressen weitergeleitet, die Sie in Target IP addresses (Ziel-IP-Adressen) festlegen. Weitere Informationen finden Sie unter So bestimmt Resolver, ob der Domainname in einer Abfrage einer Regel entspricht.

Ausgehender Endpunkt

Resolver leitet DNS-Abfragen durch den hier angegebenen ausgehenden Endpunkt an die IP-Adressen weiter, die Sie in Target IP addresses (Ziel-IP-Adressen) festlegen.

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- oder IPv6-Adressen und die Protokolle an, die Sie für den Endpunkt verwenden möchten.

Tags

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 denen Sie AWS Billing and Cost Management Ihre Rechnung organisieren können. AWS Weitere Informationen zur Verwendung von Tags für die Kostenzuordnung finden Sie unter Verwenden von Kostenzuordnungs-Tags im AWS Billing -Benutzerhandbuch.

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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

   Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

   Betriebsbereit

   Die Amazon-VPC-Netzwerkschnittstellen für diesen Endpunkt sind ordnungsgemäß konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und Resolver weitergeben.

   Aktualisieren

   Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

   Automatische Wiederherstellung

   Resolver versucht die Wiederherstellung einer oder mehrerer Netzwerkschnittstellen, 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 bei Route 53 Resolver.

Aktion erforderlich

Dieser Endpunkt ist fehlerhaft, und Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zuordnen. 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. Dies sind die beiden häufigsten 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 in der Kontrolle von ist.

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-Abfragen von Ihrem Netzwerk nicht mehr an Resolver in der im Endpunkt angegebenen VPC weitergeleitet.

So löschen Sie einen eingehenden Endpunkt

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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).

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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

   Resolver erstellt und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

   Betriebsbereit

   Die Amazon-VPC-Netzwerkschnittstellen für diesen Endpunkt sind ordnungsgemäß konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und Resolver weitergeben.

   Aktualisieren

   Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

   Automatische Wiederherstellung

   Resolver versucht die Wiederherstellung einer oder mehrerer Netzwerkschnittstellen, 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 bei Route 53 Resolver.

   Aktion erforderlich

   Dieser Endpunkt ist fehlerhaft, und Resolver kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zuordnen. 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. Dies sind die beiden häufigsten 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 in der Kontrolle von ist.

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, leitet Resolver nicht länger DNS-Abfragen für Regeln, die den gelöschten ausgehenden Endpunkt angeben, von Ihrer VPC an Ihr Netzwerk weiter.

So löschen Sie einen ausgehenden Endpunkt

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Resolver Abfragen für bestimmte Domainnamen an Ihr Netzwerk weiterleitet, erstellen Sie eine Weiterleitungsregel für alle 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

So erstellen Sie Weiterleitungsregeln und verknüpfen diese mit einer oder mehreren VPCs

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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? Amazon Route 53 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 diese mit einer oder mehreren VPCs verknüpfen. Die Regeln funktionieren erst, nachdem sie einer VPC zugeordnet wurden. Wenn Sie eine Regel mit einer VPC verknüpfen, beginnt Resolver damit, DNS-Abfragen für den in der Regel angegebenen Domainnamen an die in der Regel angegebenen DNS-Resolver weiterzuleiten. Die Abfragen durchlaufen den ausgehenden Endpunkt, den Sie beim Erstellen der Regel angegeben haben.

So verknüpfen Sie eine Weiterleitungsregel mit einer oder mehreren VPCs

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 mindestens einer VPCs zuordnen möchten.
5. Wählen Sie Associate VPC (VPC zuordnen) aus.
6. Wählen Sie unter VPCs that use this rule (VPCs, die diese Regel verwenden) die VPCs aus, denen 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:

- Sie möchten, dass Resolver für DNS-Abfragen, die aus dieser VPC stammen, keine Abfragen für den in der Regel angegebenen Domainnamen mehr an Ihr Netzwerk weiterleitet.

- Sie möchten die Weiterleitungsregel löschen. Wenn eine Regel aktuell mit einer oder mehreren VPCs verknüpft ist, müssen Sie die Zuordnung der Regel zu allen VPCs aufheben, bevor Sie sie löschen können.

Wenn Sie die Zuordnung einer Weiterleitungsregel zu einer oder mehreren VPCs aufheben möchten, führen Sie die folgenden Schritte aus.

So heben Sie die Zuordnung einer Weiterleitungsregeln zu einer VPC auf

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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, deren Zuordnung zu einer oder mehreren VPCs sie aufheben 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 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 von freigegebenen Regeln zu VPCs

Wenn ein anderes AWS Konto eine oder mehrere Regeln mit Ihrem Konto gemeinsam genutzt hat, können Sie die Regeln Ihren VPCs genauso zuordnen, wie Sie Regeln zuordnen, die Sie mit Ihren 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 für andere Konten freigeben und die Regel dann entweder löschen oder die Freigabe aufheben, die Regel jedoch mit einer oder mehreren VPCs verknüpft war, beginnt Route 53 damit, DNS-Abfragen für diese VPCs basierend auf den verbleibenden Regeln zu verarbeiten. 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 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 freigegeben wurde, die Regel einer oder mehreren VPCs zuordnet, gilt der Höchstwert für die Anzahl an Zuordnungen zwischen Regeln und VPCs pro Region für das Konto, für das die Regel freigegeben wurde.

Aktuelle Resolver-Kontingente finden Sie unter Kontingente bei Route 53 Resolver.

Berechtigungen

Um eine Regel mit einem anderen AWS Konto zu teilen, benötigen Sie die Erlaubnis, 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 ein anderes AWS Konto einzusehen

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Seite Rule: ***rule name*** zeigt der Wert unter Owner (Eigentümer) die ID des Kontos an, das die Regel erstellt hat. 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.

Beschreibung

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.

Auftraggeber

Geben Sie die AWS Kontonummer, den Namen der Organisationseinheit oder den Namen der Organisation ein.

Tags

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 Billing and Cost Management 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 mit VPCs verknüpft ist, müssen Sie die Zuordnung der Regel zu den VPCs aufheben, 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 führt dazu, dass Route 53 als rekursiver Resolver für alle Domainnamen arbeitet, für die Sie keine benutzerdefinierten Regeln erstellt haben, und für die 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 im Resolver

Wenn der `enableDnsHostnames` und `enableDnsSupport` auf `true` für eine Virtual Private Cloud (VPC) von Amazon VPC eingestellt sind, erstellt der 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 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Wählen Sie im Navigationsbereich unter Resolver VPCs aus und wählen Sie dann eine VPC-ID.
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.

Die zugehörigen APIs finden Sie unter Resolver configuration APIs (Resolver-Konfigurations-APIs).

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 vom Route-53-Resolver auf öffentlich signierte Namen angewendet, wenn dieser eine rekursive DNS-Auflösung durchführt.

Wenn der Route-53-Resolver allerdings Daten an einen anderen DNS-Resolver weiterleitet, führt dieser Resolver die 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 das Amazon Route 53 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 Route 53 Resolver zwar die DNSSEC-Validierung durchführt, aber weder DNSSEC-Datensätze zurückgibt noch das AD-Bit in der Antwort festlegt. Daher wird die Durchführung Ihrer eigenen DNSSEC-Validierung derzeit vom Route 53 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/route53/.
2. Klicken Sie im Navigationsbereich, unter Resolver wählen Sie VPCs aus.
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
- Weiterleiten des Datenverkehrs an eine Amazon-EC2-Instance
- Weiterleiten des Datenverkehrs an einen Service AWS App Runner
- Weiterleiten des Datenverkehrs in 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 andere Ressourcen AWS
- Amazon Route 53 und Amazon Route 53 Resolver-Ressourcen mit AWS CloudFormation

Weiterleiten des Datenverkehrs zu einer Amazon-API-Gateway-API mithilfe des Domainnamens

Amazon API Gateway können Sie benutzen, um APIs zu erstellen, veröffentlichen, warten, überwachen und sichern. Sie können APIs erstellen, die zusätzlich zu den in der AWS Cloud gespeicherten Daten auf AWS Dienste oder andere Webdienste zugreifen.

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.

- 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.

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 erhebt keine Gebühren für Aliasabfragen an API Gateway 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:

  - Benutzerdefinierte Domainnamen für HTTP-APIs einrichten im Entwicklerhandbuch für Amazon API Gateway.
  - Benutzerdefinierte Domainnamen für REST-APIs einrichten im Entwicklerhandbuch für Amazon API Gateway.
  - Einrichtung von benutzerdefinierten Domainnamen für WebSocket APIs 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.

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 Management Console 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:

   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 Ziel-Domainnamen enthält nur APIs, die über einen benutzerdefinierten Domainnamen verfügen, 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 A – IPv4 address (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.

Weiterleitung von Traffic an eine CloudFront Amazon-Distribution mithilfe Ihres Domainnamens

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 den URLs für Ihre Inhalte verwenden, z. B.:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Alternativ können Sie Ihren eigenen Domainnamen in URLs verwenden, zum Beispiel:

```
http://example.com/logo.jpg
```

Folgen Sie den Schritten im Amazon CloudFront Developer Guide, um in den URLs Ihrer Dateien in einer CloudFront Distribution Ihren eigenen Domainnamen anstelle des Domainnamens zu verwenden, der Ihrer Distribution CloudFront zugewiesen wurde. Weitere Informationen zur Verwendung Ihres eigenen Domainnamens bei einer CloudFront Distribution finden Sie unter Verwenden benutzerdefinierter URLs durch Hinzufügen von alternativen Domainnamen (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. Fordern Sie ein öffentliches Zertifikat an, damit CloudFront Amazon-Distributionen HTTPS erfordern. Weitere Informationen finden Sie unter Schritt 2: Anfordern eines öffentlichen Zertifikats und DNS-Validierung in AWS Certificate Manager im AWS Certificate Manager - Benutzerhandbuch.
4. Eine CloudFront Distribution. Die Verteilung muss einen alternativen Domainnamen enthalten, der dem Domainnamen entspricht, den Sie für Ihre URLs verwenden möchten, und nicht dem Domainnamen, CloudFront der Ihrer Distribution zugewiesen wurde.

   Beispiel: Wenn Sie möchten, dass die URLs für Ihre Inhalte den Domainnamen example.com enthalten, muss das Feld Alternate Domain Name für die Verteilung example.com umfassen.

   Weitere Informationen finden Sie in der folgenden Dokumentation im Amazon CloudFront Developer Guide:

   - Aufgabenliste für die Erstellung einer Verteilung

- Eine Distribution mithilfe der CloudFront Konsole erstellen oder aktualisieren

Konfiguration von Amazon Route 53 für die 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 Verwenden benutzerdefinierter URLs durch Hinzufügen alternativer Domainnamen (CNAMes) im Amazon CloudFront Developer Guide.

> **Note**
>
> Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route 53-Server übertragen. Wenn die Änderungen wirksam werden, können Sie den 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 IPv6 aktiviert ist:

   a. Melden Sie sich bei der an AWS Management Console 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 General (Allgemein) im Abschnitt Settings (Einstellungen) die Option „Edit“ (Bearbeiten) aus und scrollen Sie herunter, um im IPv6-Feld zu überprüfen, ob IPv6 für die Verteilung aktiviert ist. Wenn IPv6 aktiviert ist, müssen Sie zwei Alias-Datensätze für die Verteilung erstellen: einen, um den IPv4-Datenverkehr an die Verteilung zu leiten und einen, um den IPv6-Datenverkehr weiterzuleiten. Klicken Sie auf Abbrechen.

Weitere Informationen finden Sie unter IPv6 aktivieren im Thema Werte, die Sie angeben, wenn Sie eine Distribution erstellen oder aktualisieren im Amazon CloudFront Developer Guide.

2. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
3. Klicken Sie im Navigationsbereich auf Hosted Zones (Gehostete Zonen).
4. Wählen Sie den verknüpften Namen der gehosteten Zone für die Domain aus, die Sie verwenden möchten, um den Traffic an Ihre CloudFront Distribution weiterzuleiten.
5. Wählen Sie Datensatz erstellen.

   Sie können den Assistenten verwenden, um die Datensätze zu erstellen, oder wählen Sie Wechseln zu Schnellerstellung.
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 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.

   Alias

   Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

   > **Important**
   >
   > Sie müssen einen Alias-Datensatz erstellen, damit die CloudFront Verteilung funktioniert.

Bewerten/Weiterleiten des Datenverkehrs an

Wählen Sie Alias für CloudFront Distributionen. Die Region us-east-1 ist standardmäßig ausgewählt. 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.

Datensatztyp

Wählen Sie A – IPv4 address (IPv4-Adresse).

Wenn IPv6 für die Verteilung aktiviert ist und Sie einen zweiten Datensatz erstellen, wählen Sie AAAA – IPv6 address (IPv6-Adresse) aus.

Evaluate Target Health

Übernehmen Sie den Standardwert No.

7. Wählen Sie Create records (Datensätze erstellen).
8. Wenn IPv6 für die Verteilung aktiviert ist, wiederholen Sie die Schritte 5 bis 7. Geben Sie die gleichen Einstellungen an, außer für das Feld Datensatztyp, wie in Schritt 6 erläutert.

Weiterleiten des Datenverkehrs an eine Amazon-EC2-Instance

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

Sie können den Datenverkehr für Ihre Domain, wie beispielsweise „example.com“, mithilfe von Amazon Route 53 an Ihren Server weiterleiten, wenn Sie eine Website hosten oder eine Webanwendung auf einer EC2-Instance ausführen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes:

- Eine Amazon-EC2-Instance. Informationen zum Starten einer EC2-Instance finden Sie in der folgenden Dokumentation:

- Linux — Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 EC2-Linux-Instances im Amazon EC2 EC2-Benutzerhandbuch
- Microsoft Windows — Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 Windows-Instances im Amazon EC2 EC2-Benutzerhandbuch

> **Important**
>
> Wir empfehlen, dass Sie außerdem eine Elastic IP-Adresse erstellen und diese mit Ihrer EC2-Instance verknüpfen. Eine Elastic IP-Adresse stellt sicher, dass sich die IP-Adresse Ihrer Amazon EC2-Instance nicht mehr 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 finden Sie unter Amazon Route 53 zum DNS-Dienst für eine vorhandene Domäne machen.

Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an eine Amazon-EC2-Instance

Zum Konfigurieren von Amazon Route 53 zur Weiterleitung des Datenverkehrs an eine EC2 Instance führen Sie die folgenden Schritte aus.

So leiten Sie den Datenverkehr an eine Amazon-EC2-Instance

1. Rufen Sie die IP-Adresse für die Amazon-EC2-Instance ab:

   a. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie 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. Notieren Sie sich im unteren Bereich der Registerkarte Description den Wert von Elastic 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 Datenverkehr an die EC2-Instance 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 EC2-Instance zu leiten, 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 Sie A – IPv4 address (IPv4-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 Übertragung abgeschlossen ist, können Sie den Datenverkehr an die EC2-

Instance leiten, indem Sie den Namen des Datensatzes angeben, 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 Service AWS App Runner

AWS App Runner ist ein vollständig verwalteter Service, der es Entwicklern leicht macht, containerisierte Webanwendungen und 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

   Übernehmen Sie den Standardwert A – IPv4 address.

   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 den App-Runner-Dienst leiten, indem Sie den Namen des Alias-Datensatzes angeben, den Sie in diesem Verfahren erstellt haben.

Weiterleiten des Datenverkehrs in 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 Elastic Beanstalk Beanstalk-Konsole an AWS Management Console und öffnen Sie sie 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 Management Console 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 Route 53-Konsole an AWS Management Console 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

   Übernehmen Sie die Standardeinstellung A – Ipv4 address (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 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 Amazon-EC2-Instances hosten, können Sie den Datenverkehr auf Ihrer Website mithilfe eines Elastic-Load-Balancing-Load-Balancers (ELB) an alle 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 Route 53-Konsole an AWS Management Console 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 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 Subdomainnamen (www.example.com) anfordert, kann der Client eine IPv4-Adresse (einen A-Datensatz), eine IPv6-Adresse (einen AAAA-Datensatz) oder sowohl die IPv4- als auch die IPv6-Adresse (in getrennten Anforderungen mit IPv4) 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. Sie müssen dualstack. für Application und Classic Load Balancer aus dem anderen Konto voranstellen.

Datensatztyp

Wählen Sie A – IPv4 address (IPv4-Adresse).

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 Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

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.

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 erhebt keine Gebühren für Aliasabfragen an S3-Buckets oder andere AWS Ressourcen.

Voraussetzungen

Bevor Sie beginnen, benötigen Sie Folgendes. Wenn Sie noch nicht mit Amazon Route 53 oder S3 gearbeitet haben, finden Sie unter Erste Schritte mit Amazon Route 53 Anleitungen, die Sie durch den gesamten Prozess führen, einschließlich Registrierung eines Domainnamens und Konfiguration eines S3 Buckets.

- Ein S3-Bucket, der zum Hosten einer statischen Website konfiguriert ist.

  Weitere Informationen finden Sie unter Konfigurieren eines Buckets für Website-Hosting im Benutzerhandbuch für Amazon Simple Storage Service.

  > **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. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Route 53.

  > **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 zusätzlich zu unter Erstellen einer CloudFront Distribution und Konfiguration alternativer Domainnamen und

HTTPS im CloudFront Benutzerhandbuch. 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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:

   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 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.

Alias

Wenn Sie die Datensatzerstellungsmethode Schnell erstellen verwenden, aktivieren Sie Alias.

Bewerten/Weiterleiten des Datenverkehrs 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 vom AWS Girokonto erstellt.

Wenn Sie den Bucket mit einem anderen AWS Konto 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.

Datensatztyp

Wählen Sie A – IPv4 address (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 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 in ihren eigenen VPCs gehostet werden, 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 berechnet 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 Interface VPC Endpoints (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 Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie 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 Schnittstellen-Endpunkt 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 address (IPv4-Adresse).

Evaluate Target Health

Übernehmen Sie den Standardwert Ja.

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.

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 andere Ressourcen AWS

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.

Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers

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 Route 53 Application Recovery Controller Integritätsprüfungen für die Routingkontrolle mit DNS-Failoverdatensätzen einrichten, um Datenverkehrs-Failover für Ihre Anwendung zu verwalten. Weitere Informationen hierzu finden Sie unterAmazon Route 53 Application Recovery Controller Entwicklerhandbuchaus.

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 mit Zustandsprüfungen auch programmgesteuert über eines der AWS SDKs, die AWS Command Line Interface AWS Tools for Windows PowerShell, oder die Route 53-API arbeiten.

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.
- Bei einer Integritätsprüfung kann nur ein CloudWatch Alarm überwacht werden, der sich in demselben AWS Konto wie der Gesundheitscheck befindet.

Amazon Route 53 Application Recovery-Controller

Amazon Route 53 Application Recovery Controller gibt Ihnen Einblicke, ob Ihre Anwendungen und Ressourcen für die Wiederherstellung bereit sind, und unterstützt Sie bei der Verwaltung und Koordination des Failovers. Zustandsprüfungen in Route 53 ARC sind Routingsteuerungen zugeordnet, bei denen es sich um einfache Ein/Aus-Schalter handelt. Sie konfigurieren jede Zustandsprüfung der Routingsteuerung mit einem Failover-DNS-Eintrag. Anschließend können Sie einfach Ihre Routing-Steuerelemente in Route 53 ARC aktualisieren, um den Verkehr umzuleiten und ein Failover für Ihre Anwendungen durchzuführen, z. B. über Availability Zones oder AWS-Regionen hinweg. Weitere Informationen finden Sie unter Amazon Route 53 Application Recovery Controller Entwicklerhandbuchaus.

Weitere Informationen zur Bereitschaftsprüfungen finden Sie unter.Bereitschaftsprüfung in Route 53 ARC. Weitere Informationen zur Weiterleitung finden Sie unter Routingsteuerung in Route 53 ARC im Entwicklerhandbuch für Route 53 ARC.

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.

Themen

- So ermittelt Route 53 den Status von Zustandsprüfungen zur Überwachung eines Endpunkts
- So ermittelt Route 53 den Status von Zustandsprüfungen zur Überwachung anderer Zustandsprüfungen
- So bestimmt Route 53 den Status von Integritätsprüfungen, die Alarme überwachen CloudWatch

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. Wenn die Ressource beispielsweise für die Wartung heruntergefahren wird, leider sie unter einem verteilten Denial-of-Service-Angriff (DDoS) 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, so dass 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.

Für Zustandsprüfungen, die einen Endpunkt überwachen (mit Ausnahme von TCP-Zustandsprüfungen), müssen die Header, wenn die Antwort vom Endpunkt alle Header enthält, in dem Format vorliegen, das in RFC7230 Hypertext Transfer Protocol (HTTP/1.1): Message Syntax und Routing (Nachrichtensyntax und Routing), Abschnitt 3.2, „Header Fields“ (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. Wenn Sie die Integritätsprüfung umkehren, behandelt Route 53 einen fehlerfreien Endpunkt als fehlerhaft und umgekehrt.

So bestimmt Route 53 den Status von Integritätsprüfungen, 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 State-API-Vorgangs nicht erzwingen, dass sich der CloudWatch SetAlarmStatus 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. Wenn Sie die Integritätsprüfung umkehren, behandelt Route 53 einen fehlerfreien Endpunkt als fehlerhaft und umgekehrt.

Erstellen, Aktualisieren und Löschen von Zustandsprüfungen

Die Verfahren in den folgenden Themenabschnitten erläutern, wie Sie Route 53-Zustandsprüfungen erstellen, aktualisieren und löschen.

> **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.

Themen

Erstellen und Aktualisieren von Zustandsprüfungen

Das folgende Verfahren erläutert, wie Sie Zustandsprüfungen mit der Route 53-Konsole erstellen und aktualisieren.

So erstellen oder aktualisieren Sie eine Zustandsprüfung (Konsole)

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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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

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

Wenn Sie möchten, dass diese Zustandsprüfung einen Endpunkt überwacht, geben Sie die folgenden Werte an:

- Specify endpoint by
- Protocol

- IP address
- Host name
- Port
- Domain name
- Path

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.

Protocol (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, für den Route 53-Zustandsprüfungen durchführen soll, wenn Sie Specify endpoint by IP address auswählen.

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, Special Use IPv4 Addresses (RFC 5735, IPv4-Adressen für besondere Zwecke)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space (RFC 6598,IANA-vorbehaltener IPv4-Präfix für geteilten Adressraum).
- RFC 5156, Special-Use IPv6 Addresses (RFC 5156, IPv6-Adressen für besondere Zwecke)

Wenn der Endpunkt eine Amazon-EC2-Instance ist, empfehlen wir, dass Sie eine Elastic IP-Adresse erstellen, sie Ihrer EC2-Instance zuordnen und die Elastic IP-Adresse festlegen. 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 Amazon EC2 EC2-Benutzerhandbuch.

Wenn Sie die Amazon EC2 Instance löschen, stellen Sie sicher, dass Sie auch die Integritätsprüfung löschen, die der EIP zugeordnet ist. Weitere Informationen finden Sie unter Bewährte Methoden für Elastic IP-Adressen für 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 weiteren Wert für Port und entweder HTTP oder HTTPS für Protocol festlegen, legt Route 53 für den Endpunkt eine `Host`-Kopfzeile fest, die den Wert *`Host name`*:*`Port`* enthält.

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 durch den Domänennamen festlegen, verwendet Route 53 ausschließlich IPv4, um Zustandsprüfungen 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)

Wenn Sie möchten, dass diese Zustandsprüfung den Status anderer Zustandsprüfungen überwacht, legen Sie die folgenden Werte fest:

- Health checks to monitor
- Report healthy when
- Invert health check status

- 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.

Status der Zustandsprüfung umkehren

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.

Disabled

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 an eine bestimmte Ressource stoppen möchten, ändern Sie den Wert von Invert health check status.

> **Note**
>
> Gebühren für eine Zustandsprüfung gelten weiterhin, auch wenn die Zustandsprüfung deaktiviert ist.

Überwachung von CloudWatch-Alarmen

Wenn Sie möchten, dass mit dieser Integritätsprüfung der Alarmstatus eines CloudWatch Alarms überwacht wird, geben Sie die folgenden Werte an:

- CloudWatch alarm
- Health check status
- Invert health check status
- 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 Create (Erstellen) aus. 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 Zustandsprüfung umkehren

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.

Disabled

Stoppt die Ausführung von Zustandsprüfungen durch Route 53. Wenn Sie eine Zustandsprüfung deaktivieren, stoppt Route 53 die Überwachung der entsprechenden CloudWatch Metriken.

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 an eine bestimmte Ressource stoppen möchten, ändern Sie den Wert von Invert health check status.

> **Note**
>
> Gebühren für eine Zustandsprüfung gelten weiterhin, auch wenn die Zustandsprüfung deaktiviert ist.

Erweiterte Konfiguration (nur "Monitor an endpoint")

Wenn Sie die Option für die Überwachung eines Endpunkts auswählen, können Sie auch die folgenden Einstellungen festlegen:

- Request interval
- Failure threshold
- String matching
- Search string
- Latency graphs
- Enable SNI
- Health checker regions
- Invert health check status
- Disabled

Anforderungsintervall

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. Damit kann der Endpunkt auf die HTTPS-Anforderung mit dem entsprechenden SSL/TLS-Zertifikat reagieren.

Einige Endpunkte verlangen, dass HTTPS-Anforderungen den Hostnamen in die Nachricht `client_hello` einfügen. Wenn Sie SNI nicht aktivieren, ist der Status der Zustandsprüfung `SSL alert handshake_failure`. Eine Zustandsprüfung kann diesen Status auch aus anderen

Gründen 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 umfasst einen Domainnamen im Feld `Common Name` und möglicherweise weitere im Feld `Subject Alternative Names`. 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 Zustandsprüfung umkehren

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. Weitere Informationen zu Zustandsprüfungen, die einen Zeichenfolgenabgleich durchführen, finden Sie unter String matching.

Disabled

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 an eine bestimmte Ressource stoppen möchten, ändern Sie den Wert von Invert health check status.

> **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 UpdateHealthSie unter Einchecken in der Amazon Route 53 API-Referenz.

Um einen Integritätscheck mit neuen CloudWatch Alarmeinstellungen zu aktualisieren (Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

Löschen von Zustandsprüfungen

Um Zustandsprüfungen zu löschen, führen Sie die folgenden Schritte aus.

> **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.

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

In Amazon EC2 fungieren Sicherheitsgruppen als Firewall. Weitere Informationen finden Sie unter Amazon EC2-Sicherheitsgruppen im Amazon EC2 EC2-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 Amazon EC2 EC2-Instance oder -Ressource zugelassen `<region>` wird. Wenn Sie Route-53-Zustandsprüfungen verwenden, um IPv6-Endpunkte zu überprüfen, müssen Sie auch eingehenden Datenverkehr von `com.amazonaws.<region>.ipv6.route53-healthchecks` zulassen.

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.

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 einstellen und automatische Benachrichtigungen erhalten, wenn sich der Status Ihrer Zustandsprüfungen 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.

So zeigen Sie den Status und letzten Grund für den Ausfall einer Zustandsprüfung an (Konsole)

1. Melden Sie sich bei der AWS Management Console an 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 eine Zustandsprüfung erstellen und sich dafür entscheiden, den Status eines Endpunkts zu überwachen (nicht den Status anderer Zustandsprüfungen), und wenn Sie die Option Latency graphs (Latenzdiagramme) auswählen, können Sie die folgenden Werte in CloudWatch-Diagrammen auf der Route 53-Konsole sehen:

- 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.

Zur Anzeige der Latenz zwischen Route 53-Zustandsprüfern und Ihrem Endpunkt (Konsole)

1. Melden Sie sich bei der AWS Management Console an 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 für die Daten ausführt.

   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 integrieren mit CloudWatch-Metriken, 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 Sie CloudWatch so, dass eine Amazon-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.

- So zeigen Sie den Status einer Zustandsprüfung an (Konsole)
- So erhalten Sie eine Amazon-SNS-Benachrichtigung, wenn bei der Zustandsprüfung der Status fehlerhaft ist (Konsole)
- So zeigen Sie den CloudWatch-Alarmstatus an und bearbeiten Alarme für Amazon Route 53 (Konsole)
- So zeigen Sie Route 53-Metriken mithilfe der Amazon CloudWatch-Konsole an

So zeigen Sie den Status einer Zustandsprüfung an (Konsole)

1. Melden Sie sich bei der AWS Management Console an 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 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 für die Daten ausführt.

   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
  
  .

So erhalten Sie eine Amazon-SNS-Benachrichtigung, wenn bei der Zustandsprüfung der Status fehlerhaft ist (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 Create Alarm (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 möchten, dass CloudWatch Benachrichtigungen zu einem vorhandenen SNS-Thema senden soll, wählen Sie das Thema aus der Liste aus.

   Wenn Sie möchten, dass CloudWatch zwar Benachrichtigungen senden soll, aber nicht zu einem vorhandenen SNS-Thema, gehen Sie wie folgt vor:

- Wenn Sie möchten, dass CloudWatch E-Mail-Benachrichtigungen sendet - Wählen Sie New SNS topic (Neues SNS-Thema) und setzen Sie den Vorgang fort.
- Wenn Sie möchten, dass CloudWatch Benachrichtigungen mit einer anderen Methode sendet - Öffnen Sie ein neues Browserfenster, gehen Sie zur Amazon-SNS-Konsole 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 Latenz (TCP connection time (TCP-Verbindungszeit), Time to complete SSL handshake (Zeit bis zum Abschluss des SSL-Handshake), Time to first byte (Zeit zum ersten Byte)) basieren, ob CloudWatch die Latenz für Route 53-Zustandsprüfungen in einer bestimmten Region oder für alle Regionen (Global) berechnen soll.

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 CloudWatch einen Alarm auslösen soll.

Alarmziel	Empfohlene Bedingung	Beschreibung
Status der Zustandsprüfung	Minimum < 1	Route 53-Zustandsprüfungen erstellen einen Bericht, wenn der Endpunkt fehlerhaf t ist.

Alarmziel	Empfohlene Bedingung	Beschreibung
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.
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*** Minuten/Stunden/Tag

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, damit Sie CloudWatch-Benachrichtigungen empfangen.

So zeigen Sie den CloudWatch-Alarmstatus an und bearbeiten Alarme für Amazon Route 53 (Konsole)

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 Liste CloudWatch Alarms (CloudWatch-Alarme) 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 erfasst, um zu erkennen, dass der Endpunkt nicht den Schwellenwert für den Alarm erfüllt.

   UNZUREICHENDE DATEN

   CloudWatch hat nicht genügend Statistiken aus Zustandsprüfungen erfasst, um zu erkennen, ob der Endpunkt den Schwellenwert für den Alarm erfüllt. Dies ist der erste Status eines neuen Alarms. Der Alarmstatus ändert sich auch in UNZUREICHENDE DATEN, wenn CloudWatch-Metriken 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 zu bestimmen, dass der Endpunkt die Schwellenwerte für den Alarm erfüllt, und sendet eine Benachrichtigung an die angegebene E-Mail-Adresse.

4. Zum Anzeigen und Bearbeiten von Einstellungen für einen Alarm, wählen Sie den Namen des Alarms.
5. Wenn Sie einen Alarm in der CloudWatch-Konsole anzeigen möchten, um detaillierte Informationen über den Alarm (z. B. einen Verlauf der Alarmaktualisierungen und Statusänderungen) zu erhalten, wählen Sie in der Spalte More Options (Weitere Optionen) für den Alarm die Option View (Anzeigen) aus.
6. Wenn Sie alle CloudWatch-Alarme, die Sie mit dem aktuellen AWS-Konto erstellt haben, anzeigen möchten, einschließlich der Alarme für andere AWS-Services, wählen Sie View All CloudWatch Alarms (Alle CloudWatch-Alarme anzeigen) aus.
7. Wenn Sie alle verfügbaren CloudWatch-Metriken einschließlich der Metriken, die nicht vom aktuellen AWS-Konto verwendet werden, anzeigen möchten, wählen Sie View All CloudWatch Metrics (Alle CloudWatch-Metriken anzeigen) aus.

So zeigen Sie Route 53-Metriken mithilfe der Amazon CloudWatch-Konsole an

1. Melden Sie sich bei AWS Management Console an 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.

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 Datenverkehr basierend auf dem Instance-Typ zu 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

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 Domänennamen (z. B. example.com) oder Subdomänennamen (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 Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr.

   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 Aliasdatensätze erstellen können, z. B. Amazon-EC2-Server und E-Mail-Server, die in Ihrem Rechenzentrum ausgeführt werden. 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 Aliasdatensätze, die den Datenverkehr zu AWS-Ressourcen wie ELB-Load Balancern und CloudFront-Verteilungen weiterleiten. 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 bei einigen 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 des Zustands von EC2-Instances und anderen Ressourcen (Nicht-Aliasdatensätze)

Wenn Sie Datenverkehr zu Ressourcen weiterleiten, für die Sie keine Aliasdatensätze erstellen können, z. B. EC2-Instances, erstellen Sie einen Datensatz und eine Zustandsprüfung für jede einzelne 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.

Bewerten des Zustands einer AWS-Ressource (Aliasdatensätze)

Wenn Sie Aliasdatensätze für die Weiterleitung von Datenverkehr zu ausgewählten AWS-Ressourcen verwenden, z. B. ELB-Load Balancern, können Sie Route 53 so konfigurieren, dass der Zustand der Ressource ausgewertet und Datenverkehr nur zu Ressourcen weitergeleitet wird, die fehlerfrei sind. 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. Erstellen Sie Zustandsprüfungen für die Ressourcen, für die Sie keine Aliasdatensätze erstellen können, z. B. EC2-Instances 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 über IP-Adressen, für die Sie keine Zustandsprüfungen erstellen können, finden Sie unter RFC 5735, Special Use IPv4-Adressen und RFC 6598 IANA-Reserved IPv4-Präfix für Shared-Adressraum.

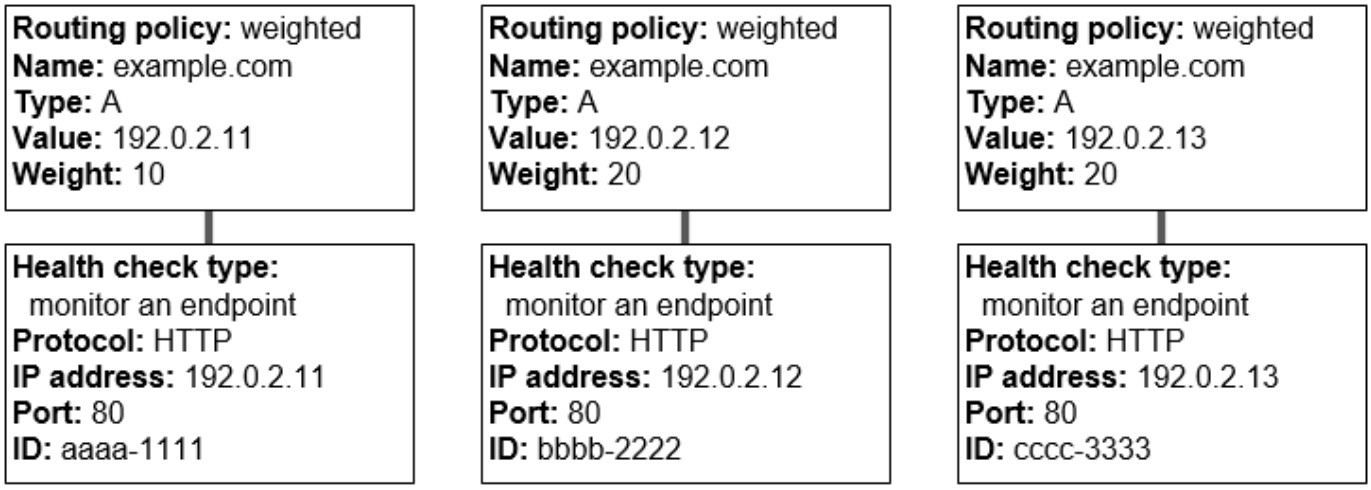
Weitere Informationen zum Erstellen von Zustandsprüfungen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

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 konfigurieren, um den Status anderer Systemdiagnosen oder die Datenströme für CloudWatch-Alarme zu überwachen. Weitere Informationen finden Sie unter Arten von Amazon Route 53-Zustandsprüfungen.

Wenn Route 53 eine Abfrage für example.com erhält, geschieht Folgendes:

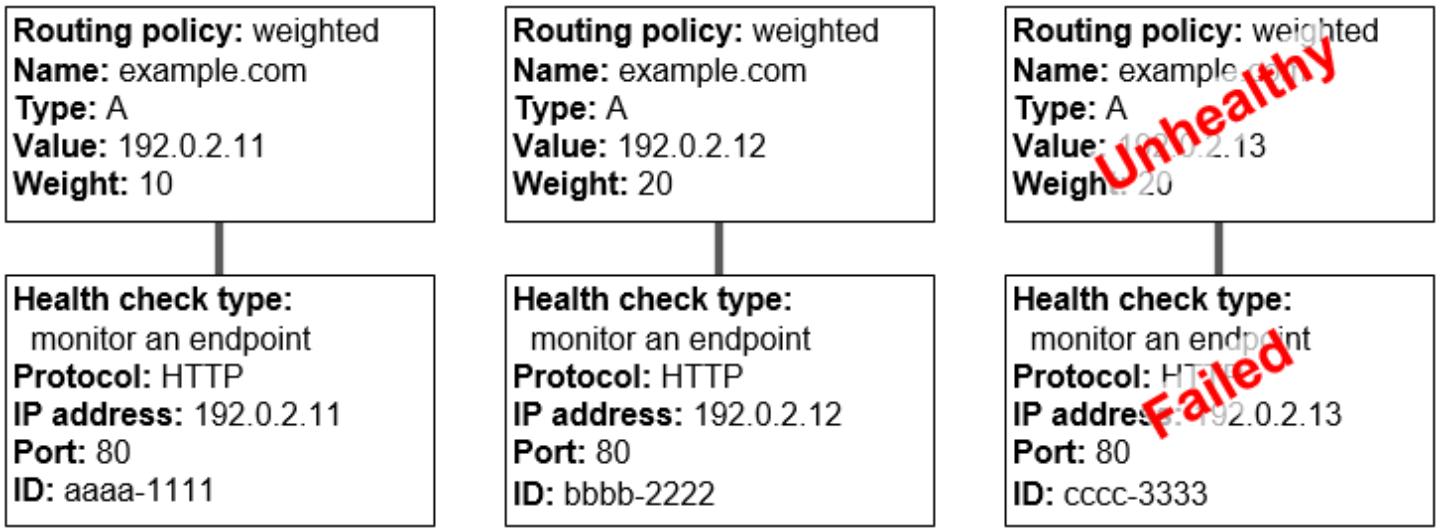
1. Route 53 wählt einen Datensatz basierend auf der Weiterleitungsrichtlinie aus. In diesem Fall wird ein Datensatz basierend auf der Gewichtung ausgewählt.
2. Der aktuelle Zustand des ausgewählten Datensatzes wird durch die Überprüfung des Status der Zustandsprüfung für den jeweiligen Ressourcendatensatz 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.

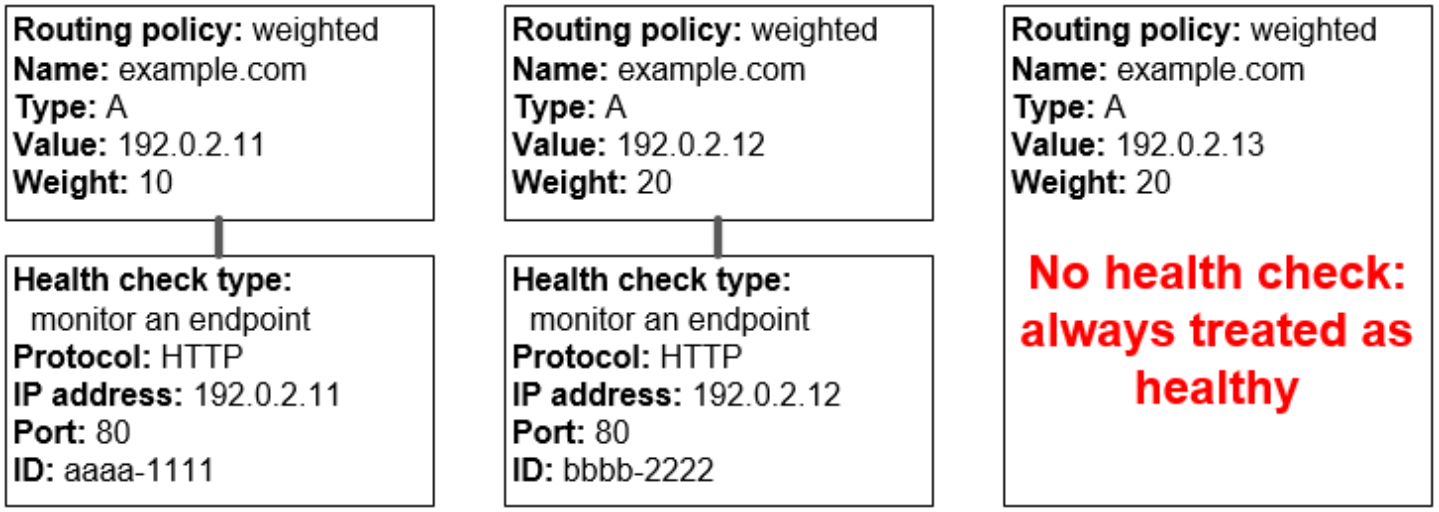
4. Wenn Route 53 einen fehlerfreien Datensatz findet, antwortet es auf die Abfrage mit dem entsprechenden Wert, z. B. der IP-Adresse in einem A-Datensatz.

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).



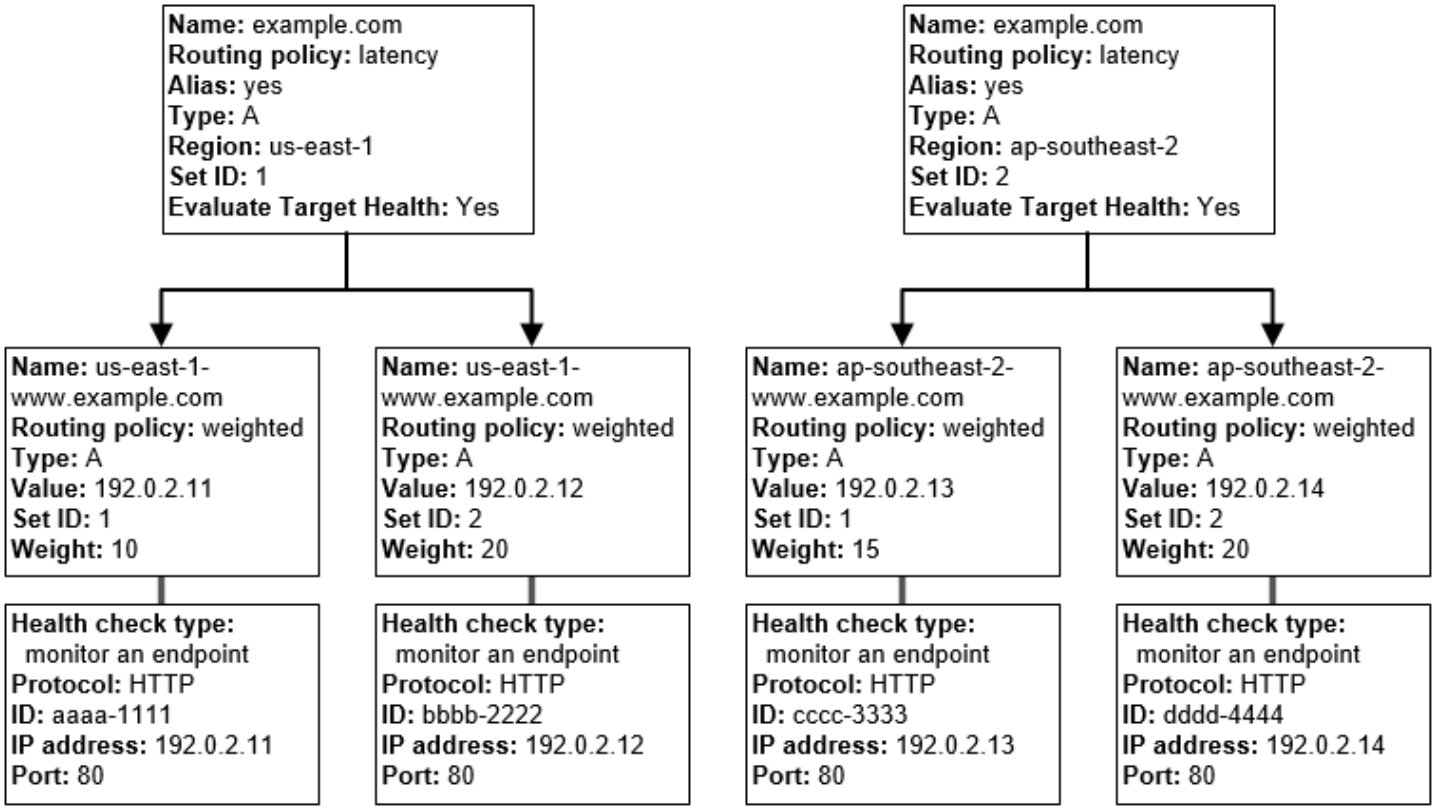
Wenn Sie eine Zustandsprüfung von einem oder mehreren Datensätzen in einer Gruppe von Datensätzen auslassen, hat Route 53 keine Möglichkeit, den Zustand der entsprechenden Ressource zu ermitteln. Route 53 bewertet diese Datensätze als fehlerfrei.



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 jeweils zwei EC2-Instances in zwei Regionen, us-east-1 und ap-southeast-2. Sie wollen, dass Route 53 Datenverkehr an Ihre EC2-Instances weiterleitet, wenn sie fehlerfrei sind, daher erstellen Sie für jede Instance eine Zustandsprüfung. 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

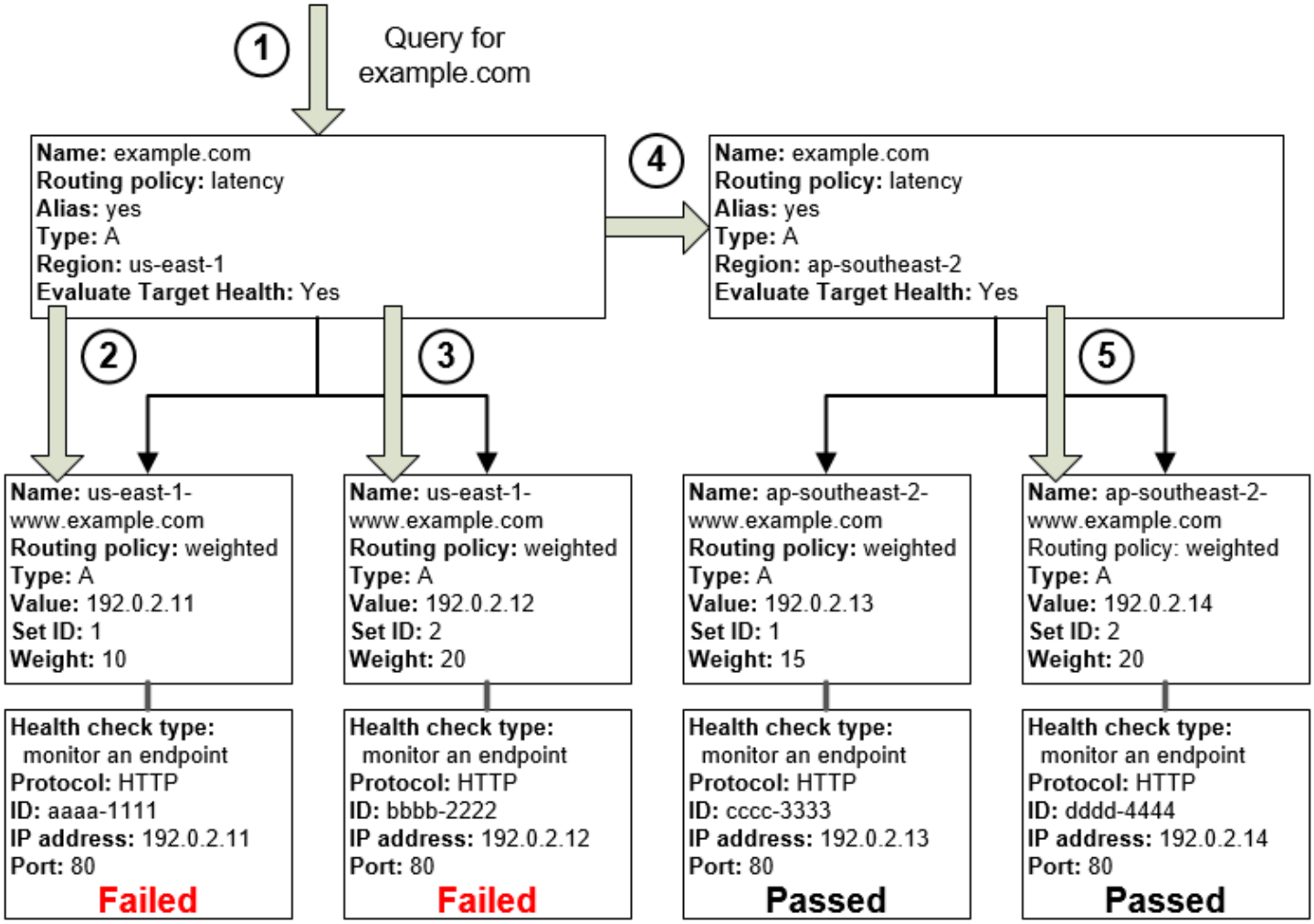
Datensätzen die Namen geben, die Ihre Benutzer verwenden werden, um auf Ihre Website oder Webanwendung zuzugreifen, z. B. example.com.

- 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?

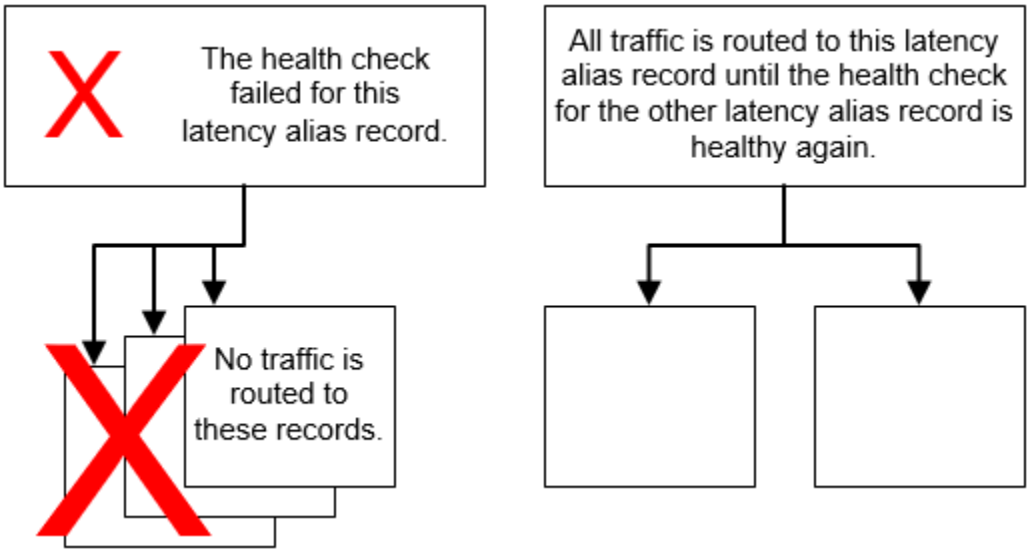
Sie können eine Zustandsprüfung mit einem Aliasdatensatz verknüpfen und/oder den Wert für Evaluate Target Health auf Yes festlegen. Es ist in der Regel jedoch nützlicher, wenn Route 53 Abfragen basierend auf dem Zustand der zugrundeliegenden Ressourcen beantwortet. d. h. der HTTP-Server, der Datenbankserver 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:

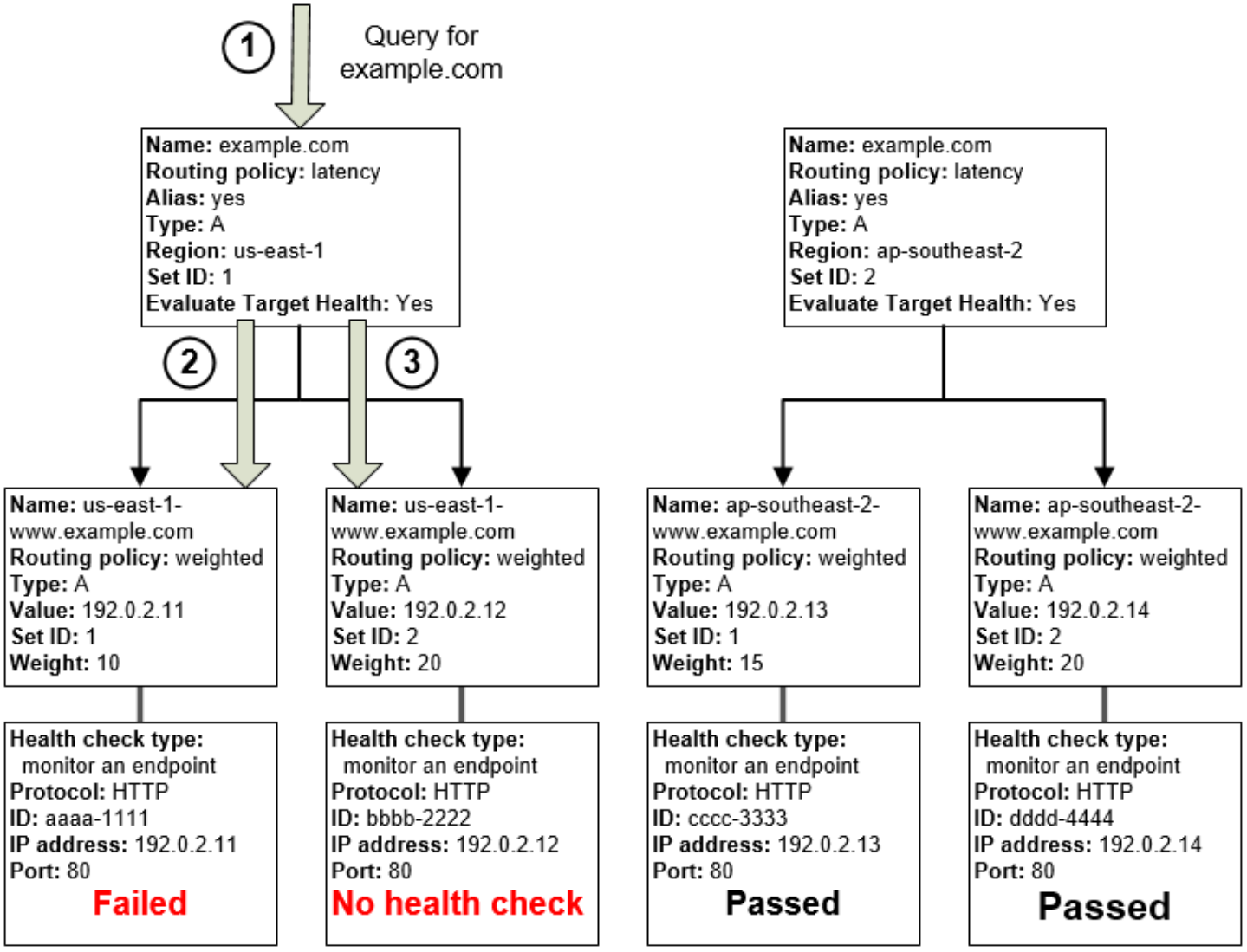
- Die dem Latenz-Aliasdatensatz zugeordnete Zustandsprüfung muss erfolgreich sein.
- Mindestens ein gewichteter Ressourcendatensatz muss als fehlerfrei bewertet werden, weil er entweder einer bestandenen Zustandsprüfung zugeordnet ist oder weil er keiner Zustandsprüfung zugeordnet ist. Im zweiten Fall 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:

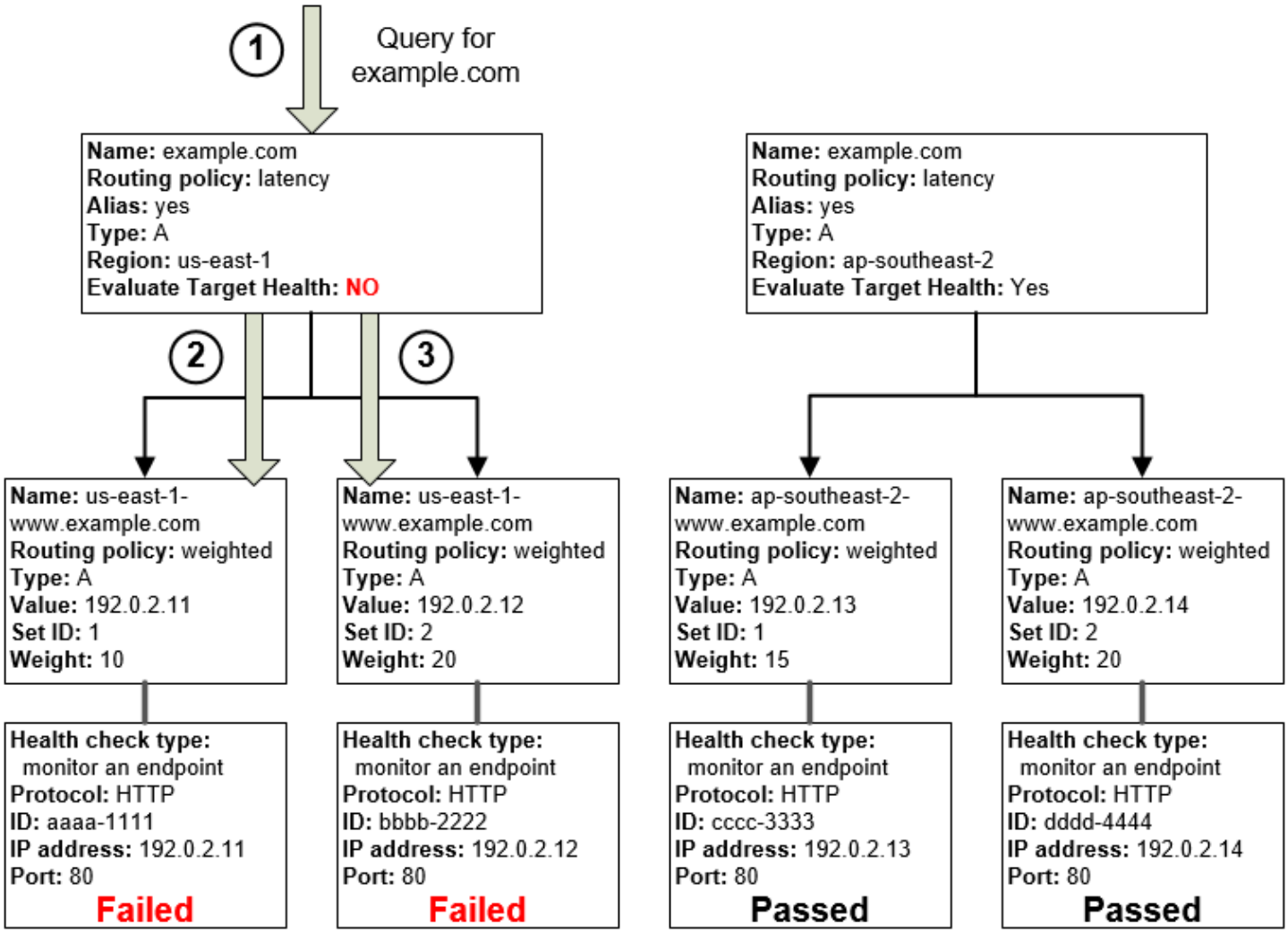
1. Route 53 erhält eine Abfrage für example.com. Basierend auf der Latenz für den Benutzer, der die Abfrage sendet, wählt Route 53 den Latenz-Aliasdatensatz für die Region us-east-1 aus.
2. Route 53 sucht das Aliasziel für den Latenz-Aliasdatensatz und prüft den Status der entsprechenden Zustandsprüfungen. 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 Zustandsprüfung für jede Ressource, zu der Datenverkehr geleitet werden soll, z. B. einer EC2-Instance oder einem Webserver in Ihrem Rechenzentrum.

> **Note**
>
> Wenn Sie Datenverkehr zu AWS-Ressourcen leiten, für die Sie Aliasdatensätze erstellen, legen Sie keine Zustandsprüfungen für diese Ressourcen an. 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 keine Aliasdatensätze erstellen können, geben Sie Yes bei 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 keine Aliasdatensätze erstellen können, geben Sie Yes bei 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 Zustandsprüfung erstellen, die auf dem Datenstrom für den Alarm basiert. Sie können beispielsweise eine CloudWatch-Metrik erstellen, die den Status der EC2-Metrik `StatusCheckFailed` überprüft, der Metrik einen Alarm hinzufügen und dann eine Zustandsprüfung erstellen, die auf dem Datenstrom für den Alarm basiert, um Instances innerhalb einer Virtual Private Cloud (VPC) zu überprüfen, die nur über private IP-Adressen verfügen. Weitere Informationen zum Erstellen von CloudWatch-Metriken und -Alarmen mithilfe der CloudWatch-Konsole finden Sie im Amazon CloudWatch-Benutzerhandbuch.

Weitere Informationen finden 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

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 Route 53-Standorte unterschiedliche Schlussfolgerungen über den Zustand eines Endpunkts ziehen, der sich von dem von CloudWatch gemeldeten Zustand unterscheidet. Die Route 53-Zustandsprüfungen in jeder AWS-Region senden ständig Status von Zustandsprüfungen an alle -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 Billing and Cost Management 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, Aktualisieren und Löschen 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
- 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.

Topics

So fügen Sie Tags zu Zustandsprüfungen hinzu (Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 (Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console 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 (Konsole)

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console 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 Add/Edit Tags das *X* neben dem Tag aus, den 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.

Route 53 Resolver DNS Firewall

Mit der Route-53-Resolver-DNS-Firewall können Sie ausgehenden DNS-Datenverkehr für Ihre virtuelle private Cloud (VPCs, Virtual Private Clouds) 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-Anforderungen von Ihren VPCs. Diese Anforderungen leiten über Resolver für die Auflösung von Domainnamen. 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 Amazon-EC2-Instance-Namen blockieren.

Die DNS-Firewall ist ein Feature von Route 53 Resolver und erfordert keine zusätzliche Einrichtung des Resolvers.

AWS Firewall Manager unterstützt DNS-Firewall

Sie können Firewall Manager verwenden, um Ihre DNS-Firewall-Regelgruppenzuordnungen für Ihre VPCs in Ihren Konten in AWS Organizations zentral zu konfigurieren und zu verwalten. Firewall Manager fügt automatisch Zuordnungen für VPCs hinzu, die in den Geltungsbereich Ihrer Firewall Manager-DNS-Firewall-Richtlinie fallen. Weitere Informationen finden Sie AWS Firewall Managerim AWS Shield Advanced Entwicklerhandbuch AWS WAF AWS Firewall Manager,, und.

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 Resolver von Anwendungen innerhalb Ihrer VPCs durchlaufen. Sie können die DNS-Firewall auch so konfigurieren, dass benutzerdefinierte Antworten für Abfragen an blockierte Domainnamen gesendet werden.
- Die Network Firewall bietet Filterung für den Datenverkehr auf Netzwerk- und Anwendungsebene, hat jedoch keine Einsicht in Abfragen, die von Route 53 Resolver durchgeführt werden.

Weitere Informationen finden über Network Firewall im Network-Firewall-Entwicklerhandbuch.

Funktionsweise der Route-53-Resolver-DNS-Firewall

Mit der Route-53-Resolver-DNS-Firewall können Sie den Zugriff auf Sites steuern und Bedrohungen auf DNS-Ebene für DNS-Abfragen, die über den Route 53 Resolver von Ihrer VPC ausgehen, blockieren. Mit DNS Firewall definieren Sie Filterregeln für Domainnamen in Regelgruppen, die Sie Ihren VPCs zuordnen. Sie können Listen von Domainnamen angeben, die Sie zulassen oder blockieren möchten, und Sie können die Antworten für die blockierten DNS-Abfragen anpassen. Sie können die Domänenlisten 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.

Route-53-Resolver-DNS-Firewall-Komponenten und -Einstellungen

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 verknüpfen dann die Regelgruppe mit einer oder mehreren VPCs. Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, aktivieren Sie die DNS-Firewall-Filterung für die VPC. Wenn Resolver dann eine DNS-Abfrage für eine VPC erhält, mit der eine Regelgruppe verknüpft ist, übergibt Resolver die Abfrage zur Filterung an die DNS Firewall.

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 Domainliste und eine Aktion für DNS-Abfragen an, deren Domains mit den Domainspezifikationen in der Liste übereinstimmen. Sie können übereinstimmende Abfragen oder Abfragetypen für die Domänen in der Liste zulassen, blockieren oder bei entsprechenden Benachrichtigungen warnen. Sie können beispielsweise einen MX-Abfragetyp für eine oder mehrere bestimmte Domänen blockieren oder zulassen. Sie können auch benutzerdefinierte Antworten für blockierte Abfragen definieren.

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 Route-53-Resolver-DNS-Firewall-Domainlisten.

Einstellung für die Domainumleitung

Mit der Einstellung für die Domänenumleitung können Sie eine DNS-Firewallregel so konfigurieren, dass alle Domänen in der DNS-Umleitungskette (Standard) überprüft werden,

z. B. CNAME, DNAME usw., oder nur die erste Domäne und der Rest als vertrauenswürdig eingestuft wird. 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 sich dafür entscheiden, die gesamte DNS-Umleitungskette zu überprüfen, 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

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.

Verknüpfung zwischen einer DNS-Firewall-Regelgruppe und einer VPC

Definiert einen Schutz für eine VPC mithilfe einer DNS-Firewall-Regelgruppe und aktiviert die 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 Aktivieren des Route-53-Resolver-DNS-Firewall-Schutzes für Ihre VPC.

Resolver-DNS-Firewall-Konfiguration für eine VPC

Gibt an, wie Resolver den Schutz der DNS-Firewall auf VPC-Ebene behandeln soll. Diese Konfiguration gilt immer dann, wenn mindestens eine DNS-Firewall-Regelgruppe mit der VPC verknüpft ist.

Diese Konfiguration legt fest, wie Route 53 Resolver Abfragen verarbeitet, wenn die DNS-Firewall sie nicht filtern kann. Wenn Resolver auf eine Abfrage keine Antwort von der DNS-Firewall erhält, schlägt es 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 Route 53 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 Route 53 Resolver-DNS-Firewallereignissen mit Amazon EventBridge.

So filtert Route-53-Resolver-DNS-Firewall DNS-Abfragen

Wenn eine DNS-Firewall-Regelgruppe mit dem Route 53 Resolver Ihrer VPC verknüpft ist, wird der folgende Datenverkehr von der Firewall gefiltert:

- DNS-Abfragen, die innerhalb dieser VPC stammen.
- 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 mit den von Ihnen konfigurierten Regelgruppen, Regeln und anderen Einstellungen und sendet die Ergebnisse zurück an 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 finden Sie unter DNS-Firewall-Regelgruppen und -Regeln und Aktivieren des Route-53-Resolver-DNS-Firewall-Schutzes für Ihre VPC.
- Innerhalb jeder Regelgruppe wertet die DNS-Firewall die DNS-Abfrage anhand der Domainliste jeder Regel aus, bis sie eine Übereinstimmung findet oder alle Regeln erschöpft. 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 Domainliste einer Regel findet, beendet sie die Abfragebewertung und antwortet Resolver mit dem Ergebnis. Wenn die Aktion `alert` lautet, sendet die DNS-Firewall auch eine Warnung an die konfigurierten Resolver-Protokolle. Weitere Informationen finden Sie unter Regelaktionen in der DNS-Firewall und Route-53-Resolver-DNS-Firewall-Domainlisten.
- Wenn die DNS-Firewall alle Regelgruppen auswertet, ohne eine Übereinstimmung zu finden, antwortet sie wie gewohnt auf die Abfrage.

Resolver leitet die Abfrage entsprechend der Antwort von der DNS-Firewall weiter. In dem unwahrscheinlichen Fall, dass die DNS-Firewall nicht reagiert, wendet Resolver den konfigurierten DNS-Firewall-Fehlermodus der VPC an. Weitere Informationen finden Sie unter Konfiguration der DNS-Firewall-VPC.

Allgemeine Schritte für die Verwendung der Route-53-Resolver-DNS-Firewall

Um die DNS-Firewall-Filterung von Route 53 Resolver in Ihrer Amazon Virtual Private Cloud VPC zu implementieren, führen Sie die folgenden Schritte auf hoher Ebene aus.

- Definieren Sie Ihren Filteransatz und Ihre Domainlisten – Entscheiden Sie, wie Sie Abfragen filtern möchten, identifizieren Sie die benötigten Domainspezifikationen und definieren Sie die Logik, die Sie zum Auswerten von Abfragen verwenden. 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 den Spezifikationen für zulässige oder gesperrte Domains erstellen und verwalten, und Sie können Domainlisten verwenden, die für Sie AWS verwaltet werden. Informationen zu Domainlisten finden Sie unter. Route-53-Resolver-DNS-Firewall-Domainlisten
- 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 mehr als eine Regelgruppe aufteilen, um die Wiederverwendung in mehreren Filterszenarien für Ihre verschiedenen VPCs zu ermöglichen. 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 Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe.
- (Optional) Ändern der Firewall-Konfiguration für die VPC – Wenn Route-53-Resolver Abfragen blockieren soll, wenn die DNS-Firewall keine Antwort für sie zurücksendet, ändern Sie in Resolver die DNS-Firewall-Konfiguration der VPC. Weitere Informationen finden Sie unter Konfiguration der DNS-Firewall-VPC.

Verwenden von Route-53-Resolver-DNS-Firewall-Regelgruppen in mehreren Regionen

Die Route 53 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 Route 53 Resolver DNS-Firewall-Regelgruppen zwischen AWS Konten teilen.

Erste Schritte mit Route-53-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 mit den VPCs zu, auf denen Sie sie verwenden möchten.

Walled-Garden-Beispiel für Route-53-Resolver-DNS-Firewall

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Management Console 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 **`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 Seite mit den WalledGardenBeispieldetails 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 WalledGardenBeispielseite auf der Registerkarte Regeln angezeigt.
15. Wählen Sie auf der WalledGardenBeispielseite 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 Geben Sie eine Domäne pro Zeile ein 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 WalledGardenBeispielseite angezeigt.
24. Auf der WalledGardenBeispielseite können Sie auf der Registerkarte Regeln 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 beginnend mit der Einstellung mit der niedrigsten Priorität, sodass die Regel mit der niedrigsten Priorität zuerst 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 AllowSelectDomänen eine niedrigere Priorität haben.

Sie haben jetzt eine Regelgruppe, die nur bestimmte Domainabfragen zulässt. Um es zu verwenden, verknüpfen Sie es mit den VPCs, auf denen Sie das Filterverhalten verwenden möchten. Weitere Informationen finden Sie unter Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe.

Beispiel für Route-53-Resolver-DNS-Firewall-Block-Liste

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-Anforderungen über den Route-53-Resolver.

So konfigurieren Sie eine DNS-Firewall-Blockliste mithilfe des Konsolenassistenten

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Amazon VPC-Konsole an AWS Management Console und öffnen Sie sie 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 Seite mit den BlockListBeispieldetails 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. z. B. **`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 BlockListBeispielseite auf der Registerkarte Regeln angezeigt
14. Auf der BlockedListBeispielseite können Sie auf der Registerkarte Regeln 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 beginnend mit der Einstellung mit der niedrigsten Priorität, sodass die Regel mit der niedrigsten Priorität zuerst bewertet wird.

    Wählen Sie die Regelpriorität aus und passen Sie sie so an, BlockListdass sie entweder vor oder nach allen anderen Regeln, die Sie haben, ausgewertet wird. 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 Seite mit den BlockedListBeispieldetails 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 BlockedListBeispielseite können Sie auf der Registerkarte Regeln 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 beginnend mit der Einstellung mit der niedrigsten Priorität, sodass die Regel mit der niedrigsten Priorität zuerst bewertet wird.

    Wählen Sie die Regelpriorität aus und passen Sie sie an, sodass BlockList-allowMX entweder vor oder nach allen anderen Regeln, die Sie möglicherweise 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 es zu verwenden, verknüpfen Sie es mit den VPCs, auf denen Sie das Filterverhalten verwenden möchten. Weitere Informationen finden Sie unter Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe.

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 Ihre VPCs zu definieren. 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 VPCs zuordnen, um ein konsistentes Verhalten in Ihrer gesamten Organisation zu gewährleisten. Weitere Informationen finden Sie unter Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe.
- Sie können Regelgruppen für Konten freigeben, um eine konsistente DNS-Abfrageverwaltung in Ihrer gesamten Organisation zu gewährleisten. Weitere Informationen finden Sie unter Route 53 Resolver DNS-Firewall-Regelgruppen zwischen AWS Konten teilen.
- Sie können Regelgruppen unternehmensweit 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

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 Billing and Cost Management 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 Route-53-Resolver-DNS-Firewall-Domainlisten.

Einstellung für die Domainumleitung

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 Route-53-Resolver-DNS-Firewall-Komponenten und -Einstellungen.

Abfragetyp

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: Schränkt Zertifizierungsstellen ein, die SSL/TLS-Zertifizierungen für die Domain erstellen können.
- CNAME: Gibt einen anderen Domainnamen zurück.

- DS: Datensatz, der den DNSSEC-Signaturschlüssel einer delegierten Zone identifiziert.
- MX: Spezifiziert Mailserver.
- NAPTR: R egular-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 NUMBER definiert sein, wobei NUMBER zwischen 1 und 65334 liegen kann, z. B. 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 DNS64 aktiviert ist.

Aktion

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 Prüfung der Abfrage und lassen Sie sie durchlaufen.
- Alert – Beenden Sie die Prüfung der Abfrage, lassen Sie sie durchlaufen, und protokollieren Sie eine Warnung für die Abfrage in den Route-53-Resolver-Protokollen.
- Block – Beenden Sie die Prüfung der Abfrage, blockieren Sie sie, um zu ihrem beabsichtigten Ziel zu gelangen, und protokollieren Sie die Blockaktion für die Abfrage in den Route-53-Resolver-Protokollen.

  Antworten Sie mit der konfigurierten Blockantwort wie folgt:

  - NODATA – Reagieren Sie darauf, dass die Abfrage erfolgreich war, aber keine Antwort dafür verfügbar ist.
  - NXDOMAIN – Antworten Sie mit dem Hinweis, dass der Domainname der Abfrage nicht vorhanden ist.
  - OVERRIDE – Geben Sie eine benutzerdefinierte Überschreibung in der Antwort an. Diese Option erfordert die folgenden zusätzlichen Einstellungen:
    - Record value – Der benutzerdefinierte DNS-Eintrag, der als Antwort auf die Abfrage 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, die der DNS-Resolver oder Webbrowser den Überschreibungs-Datensatz zwischenspeichern und ihn als Antwort auf diese Abfrage verwenden kann, 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 in DNS-Abfrageprotokollen.

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

Befolgen Sie die Anweisungen in diesem Thema, 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

So erstellen Sie eine Regelgruppe und ihre Regeln

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Management Console 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 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

So zeigen Sie eine Regelgruppe an und aktualisieren sie

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Management Console 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 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, stellen Sie sicher, dass sie keiner VPCs zugeordnet ist.

So löschen Sie eine Regelgruppe

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Management Console 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 die Regelgruppe aus, die Sie löschen möchten, wählen Sie dann Löschen und bestätigen Sie das Löschen.

Route-53-Resolver-DNS-Firewall-Domainlisten

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 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 Domänenlisten 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 Route 53 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 Route 53 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. Weitere Informationen zu der Quelle, auf die sich die Domain in dem Ergebnis bezieht, finden Sie unter ThreatIntelligenceDetail in der GuardDuty API-Referenz. Nur Domains`ThreatIntelligenceDetail`, deren Ergebnis „Amazon“ enthält, sind in den AWS verwalteten Domainlisten enthalten.

Weitere Informationen zu Bedrohungsinformationen von Drittanbietern finden Sie unter GuardDuty Amazon-Partner.

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 AWSManagedDomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

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?
Asien-Pazifik (Mumbai)	Ja
Asien-Pazifik (Seoul)	Ja
Asien-Pazifik (Singapore)	Ja
Asien-Pazifik (Sydney)	Ja
Asien-Pazifik (Tokyo)	Ja
Region Asien-Pazifik (Osaka)	Ja
Asien-Pazifik (Jakarta)	Ja
Asien-Pazifik (Hyderabad)	Ja
Asien-Pazifik (Melbourne)	Ja
Asien-Pazifik (Hongkong)	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 (Stockholm)	Ja
Europa (Zürich)	Ja
Europa (Spain)	Ja
Südamerika (São Paulo)	Ja
USA Ost (Nord-Virginia)	Ja
USA Ost (Ohio)	Ja
USA West (Nordkalifornien)	Ja
USA West (Oregon)	Ja
Afrika (Kapstadt)	Ja
China (Peking)	Ja

Region	Sind verwaltete Domainlisten verfügbar?
China (Ningxia)	Ja
AWS GovCloud (US)	Ja
Naher Osten (Bahrain)	Ja
Naher Osten (VAE)	Ja
Israel (Tel Aviv)	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 Resolver-Protokollen die Regelgruppe und die Liste der verwalteten Domains, die den Fehlalarm verursachen. 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 in DNS-Abfrageprotokollen.
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 Domainliste im Kontext der Route-53-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 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.

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 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 Route 53 Resolver DNS-Firewall-Regelgruppen mit Amazon CloudWatchWerte in DNS-Abfrageprotokollen, undKonfigurationen für die Protokollierung von Resolver-Abfragen verwalten.

So fügen Sie eine Domainliste hinzu

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.

   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 bei der an AWS Management Console und öffnen Sie

   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, stellen Sie sicher, dass sie keiner VPCs zugeordnet ist.

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 zu löschende Domainliste aus, wählen Sie dann Löschen und bestätigen Sie den Löschvorgang.

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 Route 53 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 die DNS-Abfragen zu protokollieren, die nach DNS-Firewall-Regeln gefiltert werden, die aus Ihren VPCs stammen, 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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 VPCs erstellt haben, die der DNS Firewall zugeordnet sind, für die Sie Abfragen protokollieren möchten. Wenn Sie VPCs in mehreren Regionen haben, müssen Sie für jede Region mindestens eine Konfiguration für die Abfrageprotokollierung 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 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 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 zum Protokollieren von Abfragen

Diese Konfiguration für die Abfrageprotokollierung protokolliert DNS-Abfragen, die aus den ausgewählten VPCs stammen. Aktivieren Sie das Kontrollkästchen für jede VPC in der aktuellen Region, für die Resolver Abfragen protokollieren soll, und wählen Sie Auswählen 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.

Route 53 Resolver DNS-Firewall-Regelgruppen zwischen AWS Konten teilen

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:

Zuordnen von freigegebenen Regelgruppen zu VPCs

Wenn ein anderes AWS Konto eine Regelgruppe mit Ihrem Konto gemeinsam genutzt hat, können Sie sie Ihren VPCs zuordnen, genauso wie Sie Regelgruppen zuordnen, die Sie erstellt haben. Weitere Informationen finden Sie unter Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe.

Löschen oder Aufheben der Freigabe einer freigegebenen Regelgruppe

Wenn Sie eine Regelgruppe für andere Konten freigeben und die Regelgruppe dann entweder löschen oder die Freigabe aufheben, entfernt die DNS-Firewall alle Zuordnungen, die die anderen Konten zwischen der Regelgruppe und ihren VPCs erstellt haben.

Maximale Einstellungen für Regelgruppen und -zuordnungen

Freigegebene Regelgruppen und ihre Zuordnungen mit VPCs sind in die Anzahl der Konten enthalten, für die die Regelgruppen freigegeben werden.

Aktuelle Kontingente für DNS-Firewall finden Sie unter Route 53 Resolver DNS Firewall.

Berechtigungen

Um eine Regelgruppe mit einem anderen AWS Konto zu teilen, benötigen Sie die Berechtigung, die PutFirewallRuleGroupRichtlinienaktion 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Seite Regelgruppe: ***Regelgruppenname*** zeigt der Wert unter Owner (Eigentümer) die ID des Kontos an, das die Regelgruppe erstellt hat. 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 Regelgruppe erstellt und für das aktuelle Konto freigegeben 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.

Beschreibung

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.

Auftraggeber

Geben Sie die AWS Kontonummer, den Namen der Organisationseinheit oder den Namen der Organisation ein.

Tags

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 Billing and Cost Management 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.

Aktivieren des Route-53-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. Wenn eine VPC einer DNS-Firewall-Regelgruppe zugeordnet ist, bietet Route-53-Resolver die folgenden DNS-Firewall-Schutzmaßnahmen:

- Resolver leitet die ausgehenden DNS-Abfragen der VPC über die DNS-Firewall weiter, und die DNS-Firewall filtert die Abfragen mithilfe der zugeordneten Regelgruppen.
- 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 Resolver DNS-Abfragen für die VPC während eines Fehlers verarbeiten soll, z. B. wenn die DNS-Firewall keine Antwort auf eine DNS-Abfrage liefert.

Verwalten von Verknüpfungen zwischen Ihrer VPC und der Route-53-Resolver-DNS-Firewall-Regelgruppe

So zeigen Sie die VPC Zuordnungen einer Regelgruppe an

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.

   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 bei der an AWS Management Console 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 die Regelgruppe aus, die Sie zuordnen möchten.
5. Wählen Sie die Option View details aus. Die Regelgruppe wird angezeigt.
6. Unten sehen Sie einen Detailbereich mit Registerkarten, der Regeln und zugehörige VPCs enthält. Wählen Sie die Registerkarte Zugeordnete VPCs aus.

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 dem Tab Zugeordnete VPCs die Option VPC zuordnen.
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 wird Ihre VPC in der Registerkarte Zugeordnete VPCs aufgelistet 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 Zuordnung aufheben. Überprüfen Sie und bestätigen Sie die Aktion.

Auf der Regelgruppenseite wird Ihre VPC auf der Registerkarte Zugeordnete VPCs mit dem Status Zuordnung aufgehoben 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 Resolver Abfragen zulässt oder diese bei Fehlern blockiert, z. B. wenn die DNS-Firewall beeinträchtigt ist, nicht reagiert oder in der Zone nicht verfügbar ist. Resolver erzwingt die Firewallkonfiguration einer VPC, wenn eine oder mehrere DNS-Firewall-Regelgruppen mit der VPC verknüpft sind.

Sie können eine VPC so konfigurieren, dass sie nicht geöffnet oder nicht geschlossen wird.

- Standardmäßig wird der Fehlermodus geschlossen, was bedeutet, dass 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 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 Management Console und öffnen Sie die Resolver-Konsole unter https://console.aws.amazon.com/route53resolver/.
2. Wählen Sie im Navigationsbereich unter Resolver VPCs aus.
3. Suchen und bearbeiten Sie auf der Seite VPCs 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-Firewall-Konfiguration, indem Sie UpdateFirewallConfig aufrufen und diese aktivieren oder deaktivieren`FirewallFailOpen`.

Sie können eine Liste Ihrer VPC-Firewall-Konfigurationen über die API abrufen, indem Sie ListFirewallConfigs aufrufen.

Amazon Route 53 53-Profile

Mit Route 53 53-Profilen können Sie DNS-bezogene Route 53-Konfigurationen auf viele VPCs und in verschiedenen VPCs 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 weitergegeben, die dem Profil zugeordnet sind. Sie können ein Profil auch mit AWS-Konten denselben 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.
- Route 53 Resolver-Regeln, sowohl für die Weiterleitung als auch für das System.
- DNS-Firewall-Regelgruppen.

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 VPCs aktivieren, denen das Profil zugeordnet ist, aber die bestehende DNSSEC-Validierungskonfiguration der VPC beibehalten.

Sie können sie auch verwenden AWS CloudFormation , um konsistente DNS-Einstellungen für neu bereitgestellte VPCs 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	None	marketing.example.com	Lokale VPC

Route 53 53-Profile — Verfügbarkeit in der Region

Route 53 53-Profile sind in den meisten kommerziellen Versionen erhältlich AWS-Regionen. Die folgende Tabelle enthält eine Liste der aktuellen Verfügbarkeit.

Route 53 53-Profile — Verfügbarkeit in der Region

Region	Profile verfügbar?
Afrika (Kapstadt)	Ja
Asien-Pazifik (Hongkong)	Ja
Asien-Pazifik (Hyderabad)	Ja
Asien-Pazifik (Jakarta)	Ja
Asien-Pazifik (Melbourne)	Ja
Asien-Pazifik (Mumbai)	Ja
Region Asien-Pazifik (Osaka)	Ja
Region Asien-Pazifik (Seoul)	Ja

Region	Profile verfügbar?
Asien-Pazifik (Singapore)	Ja
Asien-Pazifik (Sydney)	Ja
Region Asien-Pazifik (Tokio)	Ja
Kanada (Zentral)	Ja
Kanada West (Calgary)	Ja
Region Europa (Frankfurt)	Ja
Region Europa (Irland)	Ja
Europa (London)	Ja
Europa (Milan)	Ja
Europa (Paris)	Ja
Europa (Spain)	Ja
Europa (Stockholm)	Ja
Europa (Zürich)	Ja
Israel (Tel Aviv)	Ja
Naher Osten (Bahrain)	Ja
Naher Osten (VAE)	Ja
Südamerika (São Paulo)	Ja
USA Ost (Ohio)	Ja
USA West (Oregon)	Ja
USA West (Nordkalifornien)	Ja

Region	Profile verfügbar?
USA Ost (Nord-Virginia)	Ja

Allgemeine Schritte zur Verwendung von Route 53 53-Profilen

Um Amazon Route 53 53-Profile in Ihren Amazon Virtual Private Cloud Cloud-VPCs zu implementieren, 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, Route 53-Resolver-Regeln (sowohl Weiterleitungs- als auch Systemregeln) sowie DNS-Firewall-Regelgruppen. Weitere Informationen finden Sie unter Ordnen Sie DNS-Firewall-Regelgruppen einem Route 53 53-Profil zuZuordnen von privaten Hosting-Zonen zu einem Route 53 53-Profil,Resolver-Regeln 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 sofort auf die VPCs 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 verknüpften VPCs deaktivieren möchten.
   - Für die Reverse-DNS-Lookup-Konfiguration von Resolver können Sie sie aktivieren, deaktivieren oder die für die VPC lokal definierten auto definierten Regeln verwenden (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 einer oder mehreren VPCs zu — Um Ihr Profil verwenden zu können, ordnen Sie es einer oder mehreren VPCs zu. Weitere Informationen finden Sie unter VPCs ein Route 53 53-Profil zuordnen.

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 VPCs zuordnen und bearbeiten, wie einige der Resolver-Konfigurationen auf die VPCs angewendet werden.

CLI

Sie können ein Profil erstellen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für verwenden. `name`

```
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

- Ordnen Sie DNS-Firewall-Regelgruppen einem Route 53 53-Profil zu
- Zuordnen von privaten Hosting-Zonen zu einem Route 53 53-Profil
- Resolver-Regeln einem Route 53 53-Profil zuordnen
- Route 53 53-Profilkonfigurationen bearbeiten
- VPCs ein Route 53 53-Profil zuordnen

Ordnen Sie DNS-Firewall-Regelgruppen einem Route 53 53-Profil zu

Wählen Sie eine Registerkarte, um DNS-Firewall-Regelgruppen mithilfe der Route 53 53-Konsole einem Route 53-Profil zuzuordnen, oder AWS CLI.

- Konsole
- CLI

Console

Um DNS-Firewall-Regelgruppen zuzuordnen

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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-id``resource-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 Hosting-Zonen zu einem Route 53 53-Profil

Gehen Sie wie in diesem Verfahren beschrieben vor, um eine private gehostete Zone einem Profil zuzuordnen.

So ordnen Sie private Hosting-Zonen zu

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 Seite Private gehostete Zonen angezeigt.

Resolver-Regeln einem Route 53 53-Profil zuordnen

Folgen Sie den Schritten in diesem Verfahren, um Resolver-Regeln einem Profil zuzuordnen.

Um Resolver-Regeln zuzuordnen

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 unterErstellen von Weiterleitungsregeln.
5. Wählen Sie Associate
6. Der Zuordnungsfortschritt wird in der Spalte Status auf der Seite mit den Resolver-Regeln angezeigt.

Route 53 53-Profilkonfigurationen bearbeiten

Nachdem Sie Ressourcen einem Profil zugeordnet haben, können Sie die Standard-VPC-Konfigurationen bearbeiten, um zu entscheiden, wie sie auf die VPCs angewendet werden.

Um Profilkonfigurationen zu bearbeiten

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

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 verknüpften VPCs ihre lokale DNSSEC-Validierungskonfiguration beibehalten.
- Aktivieren Sie die DNSSEC-Validierung

  Wählen Sie diese Option, um die DNSSEC-Validierung in allen VPCs zu aktivieren, die diesem Profil zugeordnet sind.
- Deaktivieren Sie die DNSSEC-Validierung

  Wählen Sie diese Option, um die DNSSEC-Validierung in allen VPCs zu deaktivieren, die diesem Profil zugeordnet sind.

Konfiguration der umgekehrten DNS-Suche durch den Resolver

Wählen Sie einen der folgenden Werte aus:

- Aktivieren

  Wählen Sie diese Option, um auto definierte Regeln für die umgekehrte DNS-Suche in allen zugehörigen VPCs zu erstellen.
- Nicht aktiviert

  Wählen Sie diese Option, um keine auto definierten Regeln für die umgekehrte DNS-Suche in allen zugehörigen VPCs zu erstellen.
- Lokale auto definierte Regeln verwenden — Standard

  Wählen Sie diese Option, um die lokalen VPC-Einstellungen für die umgekehrte DNS-Suche für die zugehörigen VPCs 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 zugehörigen VPCs zu schließen. 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 VPCs geöffnet zu lassen. 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 im Resolver
- Konfiguration der DNS-Firewall-VPC

VPCs ein Route 53 53-Profil zuordnen

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 VPCs zuzuordnen

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 VPCs und dann Zuordnen aus.
4. Auf der Seite „VPCs zuordnen“ können Sie bis zu 10 VPCs auswählen, die Sie zuvor erstellt haben. Wenn Sie mehr als 10 VPCs zuordnen möchten, verwenden Sie die APIs. Weitere Informationen finden Sie unter AssociateProfile.
5. Wählen Sie Associate
6. Der Zuordnungsfortschritt wird in der Spalte Status auf der VPC-Seite 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 `resource-id` verwenden:

```
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 unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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 ein Beispiel für die Ausgabe, 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 Route 53-Konsole an AWS Management Console 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 löschen möchten, und wählen Sie dann Löschen aus.

   > **Important**
   >
   > Sie können ein Profil nicht löschen, wenn es mit VPCs verknüpft ist. Wenn das Profil mit anderen geteilt wird AWS-Konto, verlieren außerdem alle VPCs, denen die Profilkonfigurationen zugeordnet sind, diese Konfigurationen.

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 mit VPCs verknüpft ist. Wenn das Profil mit anderen geteilt wird AWS-Konto, verlieren außerdem alle VPCs, denen die Profilkonfigurationen zugeordnet sind, diese Konfigurationen.

Sie können ein Profil löschen, indem Sie einen AWS CLI Befehl wie den folgenden ausführen und Ihren eigenen Wert für `profile-id` verwenden:

```
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 anzeigen und aktualisieren, die einem Amazon Route 53 53-Profil zugeordnet sind

Wählen Sie die Registerkarte Konsole, um die Ressourcenzuordnungen des Route 53 53-Profils 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 oder Resolver-Regeln.
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 ein Beispiel für eine Ausgabe, 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

So trennen Sie die Zuordnung einer Ressource, die einem Route 53 53-Profil zugeordnet ist

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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. <Profile name>Wählen Sie auf der Seite die Registerkarte für die Ressource aus, die Sie löschen möchten, entweder DNS-Firewall-Regelgruppen, Private gehostete Zonen oder Resolver-Regeln.
6. Wählen Sie auf der Registerkarte für die Ressource die Ressource aus, deren Zuordnung Sie aufheben möchten, und wählen Sie dann die Zuordnung aufheben.
7. Geben Sie im Dialogfeld „Ressourcen trennen“ ein**`confirm`**, und wählen Sie dann Zuordnung trennen aus.

VPCs anzeigen, die einem Amazon Route 53 53-Profil zugeordnet sind

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

Um VPCs anzuzeigen, die einem Profil zugeordnet sind

1. Melden Sie sich bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 zugehörigen VPCs anzeigen möchten.
5. <Profile name>Wählen Sie auf der Seite die Registerkarte VPCs aus.
6. Auf der Registerkarte für VPCs können Sie die Namen, den ARN und den Status der zugehörigen VPCs einsehen.

CLI

Sie können die VPCs auflisten, denen das Profil zugeordnet ist, indem Sie einen AWS CLI Befehl wie den folgenden ausführen:

```
aws route53profiles list-profile-associations
```

Im Folgenden finden Sie ein Beispiel für eine 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 ein Beispiel für die Ausgabe, 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 eine VPC trennen möchten.
5. <Profile name>Wählen Sie auf der Seite die Registerkarte VPCs aus.
6. Wählen Sie auf der Registerkarte VPCs 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 Disassociate aus. **`confirm`**

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 seinen VPCs zuordnen kann. In diesem Fall sind alle DNS-Ressourcen und -Konfigurationen auf den zugehörigen VPCs wirksam.
- Erteilung von Administratorberechtigungen. In diesem Fall können die Konten mit dem gemeinsamen Profil das Profil ändern und es dann ihren VPCs zuordnen. Ein Besitzer 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 gehören:

- 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, die Ihnen gehören, gemeinsam nutzen und wie Sie Ressourcen verwenden, die mit Ihnen gemeinsam genutzt werden.

Inhalt

- Aufheben der Freigabe eines geteilten Route 53 53-Profils
- Identifizieren eines gemeinsamen Route 53 53-Profils
- Zuständigkeiten und Berechtigungen für gemeinsam genutzte Route 53 53-Profile
- Fakturierung und Messung
- Kontingente für Instanzen

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 Ihnen gehört, mit anderen teilen AWS-Konto, ermöglichen Sie ihnen, die DNS-bezogenen Einstellungen des Profils auf ihre VPCs anzuwenden. Dies erleichtert die Anwendung einheitlicher DNS-Konfigurationen auf Tausende von VPCs mit minimalem Verwaltungsaufwand.

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 gemeinsam nutzen können AWS-Konten. 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Freigabe verwalten aus.
4. Sie werden zur AWS RAM Konsole weitergeleitet, wo Sie die folgenden Schritte ausführen können: Erstellen einer Ressourcenfreigabe 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 gemeinsame Nutzung eines Profils aufheben, verlieren VPCs, denen die Konfigurationen dieses Profils zugeordnet sind, diese und verwenden standardmäßig die VPC-spezifischen Konfigurationen.

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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

Berechtigungen für Konsumenten

Die Standardberechtigung für Nutzer eines geteilten Profils ist schreibgeschützt. Mit Schreibschutz können sie die zugehörigen Ressourcen sehen und sie VPCs zuordnen, sie können die Ressourcenzuordnungen jedoch nicht verwalten.

Ein Besitzer kann auch vom Kunden verwaltete Berechtigungen auf der Konsole erstellen. AWS RAM 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 der Route 53 53-Profile 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, -Services, -APIs und -Tools auf Kundenstandorte ausweitet. Dadurch können Kunden AWS-Services mit On-Premises-Workloads ausführen und dabei die gleichen Programmierschnittstellen verwenden wie in AWS-Regionen. Weitere Informationen finden Sie unter Was ist AWS Outposts? im AWS Outposts-Benutzerhandbuch.

Route 53 auf Outposts bietet zwei Funktionen:

- Einen Resolver, der alle DNS-Abfragen zwischenspeichert, die vom AWS Outposts stammen.
- Hybridkonnektivität zwischen einem Outpost und einem On-Premises-DNS-Resolver, wenn Sie ein- und ausgehende Endpunkte bereitstellen.

Weitere Informationen finden Sie unter Was ist? Amazon Route 53 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 über eine Version von AWS Outposts-Racks verfügen, die nicht mit Route 53 auf Outposts kompatibel ist, wird ein AWS-Kontoteam benachrichtigt, das Ihnen beim Upgraden von AWS Outposts hilft.

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
Route 53 Resolver	Ja. Resolver verwaltet einen lokalen Cache mit Datensätzen für Anwendungen, die in dem Outpost-Rack gehostet werden, sowie für die per Peering verbundene VPC in

Feature	Verfügbarkeit in Route 53 auf Outposts
	der AWS-Region und für alle öffentlich zugänglichen Hostnamen.
Zustandsprüfungen	Nein. Zustandsprüfungen werden über die AWS-Regio n 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. Für Endpunkte ist nur der IPv4-Endpunkttyp verfügbar.
Route 53 Resolver DNS Firewall	Nicht verfügbar.
Datenverkehrsfluss	Nicht verfügbar.

Verhalten des Route-53-Resolvers, wenn die Verbindung zwischen AWS Outposts und VPC getrennt wird

Wenn die Verbindung zwischen AWS Outposts und der AWS-Region getrennt wird, gilt für die Instance von Resolver auf Outpost Folgendes:

- 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 aufgelöst werden, wenn sie im Route-53-Resolver-Cache auf dem Outpost verfügbar sind.

Erste Schritte mit Route 53 Resolver in AWS Outposts

Nachdem Sie Ihre AWS Outposts-Racks bestellt haben und sie geliefert wurden (wie im AWS Outposts-Leitfaden unter Erstellen eines AWS Outposts und Bestellen von Outpost-Kapazitäten beschrieben), können Sie Resolver auf Outpost einrichten.

Sie können auch APIs verwenden, um Route 53 auf Outposts zu verwalten. Weitere Informationen finden Sie unter Aktionen für Resolver auf Outpost.

> **Important**
>
> Die Erstellung eines Resolver-Cache für AWS Outposts kann 30 bis 150 Minuten dauern.

Nachdem Ihre AWS Outposts-Racks geliefert wurden, können Sie Route 53 auf Outposts aktivieren.

So konfigurieren Sie Resolver auf Outpost

1. Melden Sie sich bei der AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Wählen Sie auf der Seite Resolver auf Outpost die Option Resolver erstellen aus.
5. Gehen Sie auf der Seite Resolver erstellen wie folgt vor:

   - Wählen Sie unter AWS Outposts eine Instance von AWS Outposts aus, in der Sie den Resolver erstellen möchten.
   - Geben Sie einen Namen für den Resolver in das Textfeld Resolver-Name ein.
   - Warten Sie, bis Empfohlene Instance-Typen für Resolver mit Amazon-EC2-Instances aufgefüllt wurde, und wählen Sie eine Instance aus.

     Weitere Informationen zu den Instance-Typen finden Sie unter Kontingente für Resolver auf Outpost.
   - Wählen Sie unter Anzahl der Instances die Anzahl der elastischen Schnittstellen-Instances für den VPC-Resolver aus. Der Standardwert ist „4“.

Wenn Ihre Instance von AWS Outposts über keinen Instance-Typ verfügt, der Resolver unterstützt, können Sie keinen Resolver erstellen.

6. Wählen Sie Create Resolver (Resolver erstellen) aus.

   Sie können die Erstellung des Resolvers auf der Seite Resolver auf 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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver 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.

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:

Outpost-ID

Wenn Sie den Endpunkt für einen Resolver in einer VPC von AWS Outposts erstellen, ist dies die ID von 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 ausgehenden DNS-Abfragen von Ihrem Netzwerk durchlaufen diese VPC auf dem Weg zu .

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. 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, an die DNS-Resolver in Ihrem Netzwerk DNS-Abfragen weiterleiten sollen. Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben. 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 festlegen, erstellt Amazon VPC eine Elastic Network-Schnittstelle. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente bei Route 53 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 IPv4-Adresse an. IPv6 wird nicht unterstützt.

IP-Adresse

Die IP-Adresse in Ihrem Netzwerk, an die DNS-Abfragen weitergeleitet werden sollen.

Wählen Sie, ob aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst festlegen möchten.

Wenn Sie die IP-Adresse selbst festlegen möchten, geben Sie eine IPv4-Adresse an. 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.

Das sind die Tags, die AWS Billing and Cost Management für die Strukturierung Ihrer AWS-Rechnung bereitstellt. Sie können aber auch Tags 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

Wenn Sie sich für die Verwendung entschieden und einen Route-53-Resolver konfiguriert haben, können Sie auch ein- und ausgehende Endpunkte hinzufügen, um ein- und ausgehende DNS-Abfragen Ihres On-Premises-Netzwerks aufzulösen.

So konfigurieren Sie ausgehende Endpunkte für Resolver auf Outpost

1. Melden Sie sich bei der AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver 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 eingehender Endpunkte auf einem Outpost angegeben werden.
7. Wählen Sie Endpunkt erstellen.

Werte, die beim Erstellen oder Bearbeiten ausgehender Endpunkte in einer Instance von AWS Outposts angegeben werden

Wenn Sie einen eingehenden Endpunkt erstellen oder bearbeiten, geben Sie die folgenden Werte an:

Outpost-ID

Wenn Sie den Endpunkt für einen Resolver in einer VPC von AWS Outposts erstellen, ist dies die ID von 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 ausgehenden DNS-Abfragen von Ihrem Netzwerk durchlaufen diese VPC auf dem Weg zu .

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. 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, an die DNS-Resolver in Ihrem Netzwerk DNS-Abfragen weiterleiten sollen. Aus Redundanzgründen müssen Sie mindestens zwei IP-Adressen angeben. 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 festlegen, erstellt Amazon VPC eine Elastic Network-Schnittstelle. Informationen zu dem aktuellen Höchstwerten für die Anzahl der DNS-Abfragen pro Sekunde und IP-Adresse in einem Endpunkt finden Sie unter Kontingente bei Route 53 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-Adresse enthält, an die DNS-Abfragen weitergeleitet werden sollen. Das Subnetz muss eine verfügbare IP-Adresse enthalten.

Geben Sie das Subnetz für eine IPv4-Adresse an. IPv6 wird nicht unterstützt.

IP-Adresse

Die IP-Adresse in Ihrem Netzwerk, an die DNS-Abfragen weitergeleitet werden sollen.

Wählen Sie, ob aus den verfügbaren IP-Adressen im angegebenen Subnetz eine IP-Adresse für Sie auswählen soll, oder ob Sie die IP-Adresse selbst festlegen möchten.

Wenn Sie die IP-Adresse selbst festlegen möchten, geben Sie eine IPv4-Adresse an. 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, die AWS Billing and Cost Management für Ihre AWS-Rechnung bereitstellt. Sie können auch Tags 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 So erstellen Sie Weiterleitungsregeln und verknüpfen diese mit einer oder mehreren 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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Bearbeiten aus.
5. Folgende Informationen können bearbeitet werden:
   - Der Name des 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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Details anzeigen aus.
5. Die Spalte Status auf der Seite Resolver auf Outpost enthält einen der folgenden Werte:

   Creating

   Der Resolver auf Outpost wird gerade erstellt.

   Betriebsbereit

   Der Resolver auf Outpost ist korrekt konfiguriert.

   Wird aktualisiert

   Der Resolver auf Outpost aktualisiert Instance-Typen.

   Aktion erforderlich

   Dieser Resolver ist fehlerhaft und kann nicht automatisch wiederhergestellt werden. Stellen Sie sicher, dass Resolver auf Outpost von der Instance AWS Outposts unterstützt wird, um das Problem zu lösen.

   Wird gelöscht

   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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Löschen aus.
5. Geben Sie im Dialogfeld Resolver löschen den Text **`delete`** in das Textfeld ein und wählen Sie dann 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
- Anzeigen des Status für eingehende Endpunkte
- Löschen von eingehenden Endpunkten

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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver 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 eingehender Endpunkte auf einem Outpost 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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Details anzeigen aus.
5. Die Spalte Status der Liste Eingehende Endpunkte enthält einen der folgenden Werte:

   Creating

   Resolver erstellen und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

Betriebsbereit

Die Amazon-VPC-Netzwerkschnittstellen für diesen Endpunkt sind ordnungsgemäß konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und weitergeben.

Wird aktualisiert

Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

Automatische Wiederherstellung

Resolver versucht die Wiederherstellung einer oder mehrerer Netzwerkschnittstellen, 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 bei Route 53 Resolver.

Aktion erforderlich

Dieser Endpunkt ist fehlerhaft, und kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zuordnen. 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. Dies sind die beiden häufigsten 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 in der Kontrolle von ist.

Wird gelöscht

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-Abfragen von Ihrem Netzwerk nicht mehr an in der im Endpunkt angegebenen VPC weitergeleitet.

So löschen Sie einen eingehenden Endpunkt

1. Melden Sie sich bei der AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Details anzeigen aus.
5. Aktivieren Sie das Kontrollkästchen neben dem zu löschenden Endpunkt.
6. Wählen Sie Delete (Löschen).
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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver 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 AWS Management Console an 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 auf der Navigationsleiste die Region aus, in der sich Ihre Instance von AWS Outposts befindet.
4. Aktivieren Sie das Kontrollkästchen neben dem betriebsbereiten Resolver und wählen Sie Details anzeigen aus.
5. In der Liste Ausgehende Endpunkte enthält die Spalte Status einen der folgenden Werte:

Creating

Resolver erstellen und konfiguriert eine oder mehrere Amazon VPC-Netzwerkschnittstellen für diesen Endpunkt.

Betriebsbereit

Die Amazon-VPC-Netzwerkschnittstellen für diesen Endpunkt sind ordnungsgemäß konfiguriert und können eingehende oder ausgehende DNS-Abfragen zwischen Ihrem Netzwerk und weitergeben.

Wird aktualisiert

Resolver verknüpft die Zuordnung einer oder mehrerer Netzwerkschnittstellen mit diesem Endpunkt oder hebt diese auf.

Automatische Wiederherstellung

Resolver versucht die Wiederherstellung einer oder mehrerer Netzwerkschnittstellen, 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 bei Route 53 Resolver.

Aktion erforderlich

Dieser Endpunkt ist fehlerhaft, und kann ihn nicht automatisch wiederherstellen. Um das Problem zu beheben, empfehlen wir, dass Sie jede IP-Adresse überprüfen, die Sie diesem Endpunkt zuordnen. 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. Dies sind die beiden häufigsten 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 in der Kontrolle von ist.

Wird gelöscht

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, leitet nicht länger DNS-Abfragen für Regeln, die den gelöschten ausgehenden Endpunkt angeben, von Ihrer VPC an Ihr Netzwerk weiter.

So löschen Sie einen ausgehenden Endpunkt

1. Melden Sie sich bei der AWS Management Console an 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 betriebsbereiten Resolver 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 Delete (Löschen).
6. Um zu bestätigen, dass Sie den Endpunkt löschen möchten, geben Sie den Namen des Endpunkts ein und wählen Sie dann Submit (Senden).

Amazon Route 53 und Amazon Route 53 Resolver-Ressourcen mit AWS CloudFormation

Amazon Route 53 und Amazon Route 53 Resolver sind in AWS CloudFormation integriert, einen Service, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, in der alle gewünschten AWS-Ressourcen beschrieben werden. AWS CloudFormation übernimmt dann die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre Route 53- und Route 53-Resolver-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten-Konten und -Regionen immer wieder bereitstellen.

Route 53, Route 53 Resolver und AWS CloudFormation-Vorlagen

Um Ressourcen für Route 53, Route 53 Resolver und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Route 53 unterstützt das Erstellen der folgenden -Ressourcentypen inAWS 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.

Route 53 Resolver unterstützt das Erstellen der folgenden Ressourcentypen inAWS 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 Beispiele für JSON- und YAML-Vorlagen für diese Route 53-Resolver-Ressourcen, finden Sie in der Amazon Route 53 ResolverReferenz zum RDS-Ressourcentyp im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

Codebeispiele für Route 53 unter Verwendung von AWS SDKs

Die folgenden Codebeispiele veranschaulichen, wie Sie Route 53 mit einem AWS Software Development Kit (SDK) verwenden.

Eine vollständige Liste der AWS-SDK-Entwicklerhandbücher und Code-Beispiele 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

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 Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

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

Aktionen für Route 53 unter Verwendung von AWS SDKs

Die folgenden Codebeispiele zeigen, wie einzelne Route 53-Aktionen mit AWS SDKs ausgeführt werden. Diese Auszüge rufen die Route-53-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. 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 ChangeResourceRecordSets mit einem AWS SDK oder CLI
- Verwendung CreateHostedZone mit einem AWS SDK oder CLI
- Verwendung DeleteHostedZone mit einem AWS SDK oder CLI
- Verwendung GetHostedZone mit einem AWS SDK oder CLI
- Verwendung ListHostedZones mit einem AWS SDK oder CLI
- Verwendung ListHostedZonesByName mit einem AWS SDK oder CLI
- Verwendung ListQueryLoggingConfigs mit einem AWS SDK oder CLI

Verwendung **`ChangeResourceRecordSets`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ChangeResourceRecordSets`.

CLI

AWS CLI

Um einen Ressourcendatensatz zu erstellen, zu aktualisieren oder zu löschen

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 Ressourceneintrags ab, den Sie erstellen möchten:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Grundlegende 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",
        "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

Beispiel 1: In diesem Beispiel wird ein A-Record für www.example.com erstellt und der A-Record für test.example.com von 192.0.2.3 auf 192.0.2.1 geändert. Beachten Sie, dass Werte für Datensätze vom Typ TXT 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-Ressourcendatensätze erstellt werden. 'Z222222222' ist die ID der von Amazon Route 53 gehosteten Zone, in der Sie den Alias-Ressourcendatensatz erstellen. 'example.com' ist der Zonen-Apex, für den Sie einen Alias erstellen möchten, und 'www.example.com' ist eine Subdomain, für die Sie auch 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 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 = "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-Datensätze für www.example.com erstellt. In einem Viertel der Fälle (1/ (1+3)) beantwortet Amazon Route 53 Anfragen für www.example.com mit den beiden Werten für den ersten Ressourcendatensatz (192.0.2.9 und 192.0.2.10). In drei Vierteln der Fälle (3/ (1+3)) beantwortet Amazon Route 53 Anfragen für www.example.com mit den beiden Werten für den zweiten Ressourcendatensatz (192.0.2.11 und 192.0.2.12). 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 = "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 Ressourcendatensätze dieselben Werte haben. Z1111111111111 und Z3333333333333 sind Beispiele für Hosting-Zonen-IDs für den ELB-Load Balancer, die durch den Wert von dnsName angegeben werden. 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 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 = "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-Ressourcendatensätze erstellt, einen für einen ELB-Load Balancer in der Region USA West (Oregon) (us-west-2) und einen weiteren für einen Load Balancer in der Region Asien-Pazifik (Singapur) (ap-southeast-1). 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 = "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 for PowerShellCmdlet-Referenz.

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 **`CreateHostedZone`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateHostedZone`.

CLI

AWS CLI

So erstellen Sie eine gehostete Zone

Der folgende `create-hosted-zone` Befehl fügt eine gehostete Zone hinzu, die `example.com` anhand der Anruferreferenz `2014-04-01-18:47` benannt wird. 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 Working with Hosted Zones im Amazon Route 53 53-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie CreateHostedZoneunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Erstellt eine neue gehostete Zone mit dem Namen 'example.com', die einem wiederverwendbaren Delegierungssatz zugeordnet ist. Beachten Sie, dass Sie einen Wert für den CallerReference Parameter angeben müssen, damit Anfragen, die erforderlich sind, bei Bedarf erneut versucht werden müssen, ohne dass das Risiko besteht, 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 for PowerShellCmdlet-Referenz.

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 **`DeleteHostedZone`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteHostedZone`.

CLI

AWS CLI

Um eine gehostete Zone zu löschen

Der folgende `delete-hosted-zone` Befehl löscht die Hosting-Zone mit dem Wert `id` von`Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Einzelheiten zur API finden Sie DeleteHostedZonein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Löscht die gehostete Zone mit der angegebenen ID. Sie werden zur Bestätigung aufgefordert, bevor der Befehl ausgeführt wird, sofern Sie nicht den Switch-Parameter -Force hinzufügen.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Einzelheiten zur API finden Sie unter DeleteHostedZone AWS Tools for PowerShellCmdlet-Referenz.

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 **`GetHostedZone`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetHostedZone`.

CLI

AWS CLI

Um Informationen über eine gehostete Zone zu erhalten

Mit dem folgenden `get-hosted-zone` Befehl werden Informationen über die Hosting-Zone mit dem Wert `id` von abgerufen`Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Einzelheiten zur API finden Sie GetHostedZonein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt Details der Hosting-Zone mit der ID Z1D633PJN98FT9 zurück.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Einzelheiten zur API finden Sie unter Cmdlet-Referenz. GetHostedZoneAWS Tools for PowerShell

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 Codebeispiele zeigen, wie es verwendet wird`ListHostedZones`.

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

Beispiel 1: Gibt alle Ihre öffentlichen und privaten Hosting-Zonen aus.

```
Get-R53HostedZoneList
```

Beispiel 2: Gibt alle gehosteten Zonen aus, die dem wiederverwendbaren Delegierungssatz mit der ID NZ8X2CISAMPLE zugeordnet sind

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Einzelheiten zur API finden Sie unter ListHostedZonesCmdlet-Referenz.AWS Tools for PowerShell

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 **`ListHostedZonesByName`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListHostedZonesByName`.

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 Hosting-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

Beispiel 1: Gibt alle Ihre öffentlichen und privaten Hosting-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
```

Beispiel 3: Dieses Beispiel zeigt, wie Sie die gehosteten Zonen manuell auflisten können, indem Sie zuerst ein einzelnes Element abrufen und dann zwei nacheinander iterieren, bis alle Zonen zurückgegeben wurden. Dabei werden Markereigenschaften verwendet, die nach jedem Aufruf an die Serviceantwort im Stack angehängt wurden. **`$AWSHistory`**

```
Get-R53HostedZonesByName -MaxItem 1
while ($LastServiceResponse.IsTruncated)
{
    $nextPageParams = @{
        DnsName=$LastServiceResponse.NextDNSName
        HostedZoneId=$LastServiceResponse.NextHostedZoneId
    }
    Get-R53HostedZonesByName -MaxItem 2 @nextPageParams
```

```
}
```

- Einzelheiten zur API finden Sie unter ListHostedZonesByNameCmdlet-Referenz.AWS Tools for PowerShell

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 **`ListQueryLoggingConfigs`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListQueryLoggingConfigs`.

CLI

AWS CLI

Um Konfigurationen für die Abfrageprotokollierung aufzulisten

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 Protokollierung von DNS-Abfragen im Amazon Route 53 53-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie ListQueryLoggingConfigsunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel werden alle Konfigurationen für die DNS-Abfrageprotokollierung zurückgegeben, die der aktuellen Version zugeordnet sind AWS-Konto.

```
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 for PowerShellCmdlet-Referenz.

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 mithilfe von AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Route 53-Domänenregistrierung 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 Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie eine bestimmte Aufgabe ausführen können, indem Sie mehrere Funktionen innerhalb desselben Services aufrufen.

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.

Erste Schritte

Hallo Route-53-Domainregistrierung

Die folgenden Codebeispiele veranschaulichen die ersten Schritte mit der Route-53-Domainregistrierung.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 { 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.

Codebeispiele

- Aktionen für die Route 53-Domainregistrierung mithilfe von SDKs AWS
  - 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
  - Verwendung ListPrices mit einem AWS SDK oder CLI
  - Verwendung RegisterDomain mit einem AWS SDK oder CLI
  - Verwendung ViewBilling mit einem AWS SDK oder CLI
- Szenarien für die Route 53-Domänenregistrierung mithilfe von AWS SDKs
  - Beginnen Sie mit der Route 53-Domainregistrierung mithilfe eines AWS SDK

Aktionen für die Route 53-Domainregistrierung mithilfe von SDKs AWS

Die folgenden Codebeispiele zeigen, wie einzelne Route 53-Domänenregistrierungsaktionen mit AWS SDKs durchgeführt werden. Diese Auszüge rufen die Route-53-Domainregistrierungs-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. 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 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
- Verwendung ListPrices mit einem AWS SDK oder CLI
- 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 Codebeispiele zeigen, wie es verwendet wird`CheckDomainAvailability`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter CheckDomainVerfügbarkeit in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um festzustellen, ob Sie einen Domainnamen mit Route 53 registrieren können

Der folgende `check-domain-availability` Befehl gibt Informationen darüber zurück, ob der Domainname für die Registrierung über Route 53 verfügbar `example.com` ist.

Dieser Befehl wird nur in der `us-east-1` Region ausgeführt. Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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) wie `.com` und`.jp`, aber wir unterstützen nicht alle verfügbaren TLDs. Wenn Sie die Verfügbarkeit einer Domain überprüfen und Route 53 die TLD nicht unterstützt, wird die folgende Meldung `check-domain-availability` zurückgegeben.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Eine Liste der 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 Developer Guide. Weitere Informationen zur Registrierung von Domains bei Amazon Route 53 finden Sie unter Registrierung einer neuen Domain im Amazon Route 53 Developer Guide.

- Einzelheiten zur API finden Sie unter CheckDomainVerfügbarkeit in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter CheckDomainVerfügbarkeit in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
route53DomainsClient.checkDomainAvailability(availabilityRequest)
```

```
        println("$domainSuggestion is ${response.availability}")
    }
}
```

- Einzelheiten zur API finden Sie unter CheckDomainVerfügbarkeit im AWS SDK für die Kotlin-API-Referenz.

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 Codebeispiele zeigen, wie es verwendet wird`CheckDomainTransferability`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter CheckDomainÜbertragbarkeit in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um festzustellen, ob eine Domain auf Route 53 übertragen werden kann

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 eingestellt ist`us-east-1`, 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 Übertragung der Registrierung für eine Domain auf Amazon Route 53 im Amazon Route 53 53-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie unter CheckDomainÜbertragbarkeit in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter CheckDomainÜbertragbarkeit in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- Einzelheiten zur API finden Sie unter Referenz zur CheckDomainÜbertragbarkeit im AWS SDK für die Kotlin-API.

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 **`GetDomainDetail`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetDomainDetail`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetDomainDetail in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um detaillierte Informationen zu einer bestimmten Domain zu erhalten

Der folgende `get-domain-detail` Befehl zeigt detaillierte Informationen über die angegebene Domäne an.

Dieser Befehl wird nur in der `us-east-1` Region ausgeführt. Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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.com",
    "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 unter GetDomainDetail in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetDomainDetail in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { 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 unter GetDomainDetail im AWS SDK für die Kotlin-API-Referenz.

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 Codebeispiele zeigen, wie es verwendet wird`GetDomainSuggestions`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetDomainVorschläge in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um eine Liste der vorgeschlagenen Domainnamen zu erhalten

Der folgende `get-domain-suggestions` Befehl zeigt eine Liste mit vorgeschlagenen Domainnamen an, die auf dem Domainnamen basieren`example.com`. Die Antwort enthält nur Domainnamen, die verfügbar sind. Dieser Befehl wird nur in der `us-east-1` Region ausgeführt. Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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 unter GetDomainVorschläge in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetDomainVorschläge in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
```

```
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient { 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(" ")
        }
    }
}
```

- API-Details finden Sie unter GetDomainVorschläge im AWS SDK für die Kotlin-API-Referenz.

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 Codebeispiele zeigen, wie es verwendet wird`GetOperationDetail`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetOperationDetail in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um den aktuellen Status eines Vorgangs abzurufen

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 der angegebenen Operation zurück.

Dieser Befehl wird nur in der `us-east-1` Region ausgeführt. Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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 unter GetOperationDetail in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 unter GetOperationDetail in der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
```

```
    }
}
```

- Einzelheiten zur API finden Sie unter GetOperationDetail im AWS SDK für die Kotlin-API-Referenz.

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 Codebeispiele zeigen, wie es verwendet wird`ListDomains`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .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 eingestellt ist`us-east-1`, 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 ListDomainsin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun listDomains() {
    Route53DomainsClient { 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 Codebeispiele zeigen, wie es verwendet wird`ListOperations`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .NET API-Referenz.

CLI

AWS CLI

Um den Status von Vorgängen aufzulisten, 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 Domänenregistrierungsvorgängen auf.

Dieser Befehl wird nur in der `us-east-1` Region ausgeführt. Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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 übermittelt 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 { 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.

Verwendung **`ListPrices`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListPrices`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient { 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 Codebeispiele zeigen, wie es verwendet wird`RegisterDomain`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .NET API-Referenz.

CLI

AWS CLI

Um eine Domain zu registrieren

Der folgende `register-domain` Befehl registriert eine Domäne und ruft alle Parameterwerte aus einer Datei im JSON-Format ab.

Dieser Befehl wird nur in der Region ausgeführt. `us-east-1` Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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"
}
```

Um zu bestätigen, dass der Vorgang erfolgreich war, können Sie ihn ausführen`get-operation-detail`. Weitere Informationen finden Sie unter get-operation-detail.

Weitere Informationen finden Sie unter Registrieren einer neuen Domäne im Amazon Route 53-Entwicklerhandbuch.

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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 { 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 Codebeispiele zeigen, wie es verwendet wird`ViewBilling`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Domains

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 for .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 domänenbezogenen Abrechnungsdatensätze für das Girokonto 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 Region ausgeführt. `us-east-1` Wenn Ihre Standardregion auf eingestellt ist`us-east-1`, 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 { 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.

Szenarien für die Route 53-Domänenregistrierung mithilfe von AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie allgemeine Szenarien bei der Route 53-Domänenregistrierung mit AWS SDKs implementieren. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben durch Aufrufen mehrerer Funktionen innerhalb der Route-53-Domainregistrierung ausführen können. Jedes Szenario enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Beispiele

- Beginnen Sie mit der Route 53-Domainregistrierung mithilfe eines AWS SDK

Beginnen Sie mit der Route 53-Domainregistrierung mithilfe eines AWS SDK

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

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung 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.";
        }
```

```
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for .NET -API-Referenz.
  - CheckDomainVerfügbarkeit
  - CheckDomainÜbertragbarkeit
  - GetDomainEinzelheiten
  - GetDomainVorschläge
  - GetOperationEinzelheiten
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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);
        }
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Java 2.x -API-Referenz.
  - CheckDomainVerfügbarkeit
  - CheckDomainÜbertragbarkeit
  - GetDomainEinzelheiten
  - GetDomainVorschläge
  - GetOperationEinzelheiten
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository 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 { 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 { 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 { 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 { 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 { 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 { 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 { 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 { 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 { 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 { 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.
  - CheckDomainVerfügbarkeit
  - CheckDomainÜbertragbarkeit
  - GetDomainEinzelheiten
  - GetDomainVorschläge
  - GetOperationEinzelheiten
  - 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.

Sicherheit in Amazon Route 53.

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, 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 – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. 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 außerdem, wie Sie andere AWS-Services verwenden, um Ihre Route-53-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz in der Route 53

Das AWS Modell der übergreifenden Verantwortlichkeit gilt für den Datenschutz in Amazon Route 53. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfigurations- und Verwaltungsaufgaben für die AWS-Services verantwortlich, die Sie verwenden. 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, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 AWS-Services unter Verwendung der Konsole, API, AWS CLI oder AWS-SDKs arbeiten. 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 können Sie Datenverkehr an eine Unterdomain weiterleiten, indem Sie NS-Datensätze erstellen. Wenn diese NS-Datensätze auf Route-53-Namenserver verweisen, wird erwartet, dass die Namenserver mit denen im Delegierungssatz einer gehosteten Zone übereinstimmen, die für die Unterdomain autorisierend ist. Wenn diese NS-Datensätze nicht auf die richtigen Namenserver verweisen, besteht die Gefahr, dass ein Angreifer die Unterdomain ausnutzen und die Kontrolle über sie übernehmen kann. Sie werden als hängende NS-Datensätze bezeichnet.

Wenn beispielsweise eine von Route 53 gehostete Zone für eine Unterdomain gelöscht wird, bleiben ihre NS-Datensätze möglicherweise in der übergeordneten Domain hängen. In diesem Fall könnte ein Angreifer die Unterdomain kapern, indem er auf den Namenservern der gelöschten Zone eine neue gehostete Zone erstellt. Um das zu verhindern, verfolgt Route 53 die Unterdomain-Delegierungssatzpaare nach und lässt nicht zu, dass auf diesen Namenservern neue Zonen der Unterdomain erstellt werden, solange Sie die hängenden NS-Datensätze nicht entfernt haben.

Dennoch kann es aufgrund einer Fehlkonfiguration der NS-Datensätze immer noch zu hängenden NS-Datensätzen kommen. Um dieses Risiko zu minimieren, empfehlen wir Ihnen, folgende Maßnahmen zu ergreifen:

- Stellen Sie sicher, dass die Apex-NS-Datensätze der autoritativen, von Route 53 gehosteten Zone der Unterdomain mit den für die gehostete Zone festgelegten Delegierungseinstellungen übereinstimmen. Sie können den Delegierungssatz einer gehosteten Zone über die Route-53-Konsole oder über die AWS CLI suchen. Weitere Informationen finden Sie unter Auflisten von Datensätzen oder unterget-hosted-zone.
- Aktivieren Sie die DNSSEC-Signierung für die von Route 53 gehostete Zone. DNSSEC überprüft, ob DNS-Antworten von der verbindlichen Quelle stammen, und beugt so dem entsprechenden Risiko vor. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.
- Entfernen Sie die Namenserver, die die Unterdomain nicht hosten, aus den NS-Datensätzen der Unterdomain in der übergeordneten gehosteten Zone.

  – oder –

- Ersetzen Sie die Namenserver durch die vier Namenserver in der Delegierungsgruppe der autoritativen, von Route 53 gehosteten Zone der Unterdomain. Dadurch wird das Risiko ebenfalls wirksam gemindert.

Beispiele

In den folgenden Beispielen wird davon ausgegangen, dass Sie über eine übergeordnete Domain (`parent-domain.com`) und über eine Unterdomain (`sub-domain.parent-domain.com`) verfügen. Es werden drei Szenarien mit hängenden NS-Datensätzen gezeigt und Sie erfahren, wie Sie jeweils das Risiko mindern können.

Szenario 1:

In der übergeordneten gehosteten Zone `parent-domain.com` erstellen Sie NS-Datensätze für `sub-domain.parent-domain.com` mit vier Namenservern: <ns1>, <ns2>, <ns3> und <ns4>. Die Namenserver der autoritativen Unterdomain sind <ns5>, <ns6>, <ns7> und <ns8>. Daher sind <ns1>, <ns2>, <ns3> und <ns4> jeweils hängende NS-Datensätze und es besteht die Gefahr, dass ein Angreifer die Kontrolle über „sub-domain.parent-domain.com“ erlangt. Ersetzen Sie zur Minimierung des Risikos den Unterdomain-NS-Datensatz durch <ns5>, <ns6>, <ns7> und <ns8>.

Szenario 2:

`parent-domain.com` sorgt dafür, dass NS-Datensätze vom Typ `sub-domain.parent-domain.com` auf <ns1>, <ns2>, <ns3>, <ns4>, <ns5>, <ns6>, <ns7> und <ns8> verweisen. Die Namenserver der gehosteten Zone der autoritativen Unterdomain sind <ns5>, <ns6>, <ns7> und <ns8>. Somit sind <ns1>, <ns2>, <ns3> und <ns4> wieder hängende NS-Datensätze. Entfernen Sie zur Minimierung des Risikos <ns1>, <ns2>, <ns3> und <ns4> aus den NS-Datensätzen.

Szenario 3:

Sie haben einen wiederverwendbaren Delegierungssatz: <ns1>, <ns2>, <ns3> und <ns4>. Sie erstellen einen NS-Datensatz in der übergeordneten Zone und delegieren die Unterdomain an diese Namenserver im wiederverwendbaren Delegierungssatz. Sie haben die Unterdomainzone im wiederverwendbaren Delegierungssatz jedoch nicht erstellt. Somit sind <ns1>, <ns2>, <ns3> und <ns4> hängende NS-Datensätze. Um das Risiko zu minimieren, erstellen Sie die gehostete Unterdomainzone mit dem wiederverwendbaren Delegierungssatz.

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
- Zugriffskontrolle
- Übersicht zur Verwaltung der Zugriffsberechtigungen für Amazon-Route-53-Ressourcen
- Verwenden identitätsbasierter Richtlinien (IAM-Richtlinien) für Amazon Route 53
- Verwenden von serviceverknüpften Rollen für Amazon Route 53 Resolver
- AWS verwaltete Richtlinien für Amazon Route 53
- Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle zum Verwalten von Ressourcendatensätzen
- Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine

Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS

CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen

mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) 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 Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt von der Art des Benutzers ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporäre r Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benut zeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldein formationen im Referenzh andbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltun g von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benut zerhandbuch.

Themen

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.

Verwalten 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:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Wenn Sie möchten, dass die Richtlinie auch für private gehostete Zonen gilt, müssen Sie Berechtigungen für die Verwendung der Route-53-Aktion `AssociateVPCWithHostedZone` und der beiden Amazon-EC2-Aktionen `DescribeVpcs` und `DescribeRegion` erteilen, wie im folgenden Beispiel gezeigt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegion"
            ],
            "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:

```
{
    "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:

```
{
    "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 Ihnen das Arbeiten mit Route 53 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 Alias-Datensätzen, 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

Ermöglicht Ihnen die Arbeit mit Route 53 Resolver.

`sns:ListTopics`, **`sns:ListSubscriptionsByTopic`**, **`sns:CreateTopic`**, **`cloudwatch:DescribeAlarms`**, **`cloudwatch:PutMetricAlarm`**, **`cloudwatch:DeleteAlarms`**

Ermöglicht das Erstellen, Löschen und Anzeigen von CloudWatch 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 sie nur, um eine Liste der APIs abzurufen und in der Konsole anzuzeigen.

`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 zum Verwalten von Ressourcendatensätzen.

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 beispielsweise die DNSSEC-Signatur aktiviert hat, möchte möglicherweise eine IAM-Richtlinie erstellen, die die Berechtigung für eine andere Person enthält, unter anderem Ressourcensatzdatensätze (RR) 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, Änderungen an RRs, Datenverkehrsrichtlinien und Integritätsprüfungen 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-Signierung 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, die AWS SDKs 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: Erstellen von eingehenden und ausgehenden Route-53-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.

```
{
    "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.

```
{
    "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).

```
{
    "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: Erstellen von eingehenden und ausgehenden Route-53-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 VPCs anzuzeigen.

```
{
    "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 Resolver verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Resolver verknüpft ist. Serviceverknüpfte Rollen werden von Resolver vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Resolver, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Resolver definiert die Berechtigungen

seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Resolver die 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. Dies schützt Ihre Resolver-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen 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 servicegebundenen Rolle für diesen Service anzuzeigen.

Themen

Berechtigungen von serviceverknüpften Rollen für Resolver

Resolver verwendet die serviceverknüpfte Rolle **`AWSServiceRoleForRoute53Resolver`**, um Abfrageprotokolle in Ihrem Namen bereitzustellen.

Die Richtlinie für Rollenberechtigungen erlaubt es Resolver, die folgenden Aktionen für alle Ihrer Ressourcen durchzuführen:

```
{
  "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 servicegebundene Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Resolver

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Resolver-Abfrageprotokollkonfigurationszuordnung in der Amazon-Route-53-Konsole, der AWS CLI- oder der AWS-API erstellen, erstellt 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 Funktionen verwendet. Wenn Sie den Resolver-Service vor dem 12. August 2020 verwendet haben, als dieser begann, servicebezogene Rollen zu unterstützen, hat Resolver die `AWSServiceRoleForRoute53Resolver`-Rolle 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 Resolver

Resolver verhindert die Bearbeitung der `AWSServiceRoleForRoute53Resolver` serviceverknüpften Rolle. 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 servicegebundenen Rolle im IAM-Benutzerhandbuch

Löschen einer serviceverknüpften Rolle für Resolver

Wenn Sie ein Feature oder einen Service, 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 Resolver-Service 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.

Löschen Sie die von **`AWSServiceRoleForRoute53Resolver`** verwendeten Resolver-Ressourcen wie folgt:

1. Melden Sie sich bei der AWS Management Console-Managementkonsole an 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, AWS CLI- oder AWS-API, um die `AWSServiceRoleForRoute53Resolver` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Resolver-Rollen

Resolver unterstützt die Verwendung von serviceverknüpften Rollen nicht 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 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

Name der Region	Regions-ID	Support in Resolver
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 für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete 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 Domänenregistrierung und Systemdiagnose, jedoch ohne 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.
- `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.
- `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.
- `ec2:DescribeVpcs` – Ermöglicht Ihnen 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.
- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Ermöglicht das Erstellen, Löschen und Anzeigen von CloudWatch 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 sie nur, um eine Liste der APIs abzurufen und in der Konsole anzuzeigen.

Weitere Informationen zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "route53:*",
                "route53domains:*",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeRegions",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ReadOnlyAccess

Sie können die `AmazonRoute53ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Nur-Lesen-Zugriff auf Route-53-Ressourcen, einschließlich Domänenregistrierung und Systemdiagnose, jedoch ohne 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 unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

```
{
    "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.

```
{
    "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.

```
{
    "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 uneingeschränkten Zugriff auf Route-53-Resolver-Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53resolver:*` – Ermöglicht das Erstellen und Verwalten von 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 Ihnen 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
```

```
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonRoute 53 ResolverReadOnlyAccess

Sie können die `AmazonRoute53ResolverReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Nur-Lesen-Zugriff auf Route-53-Resolver-Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `route53resolver:Get*`— Ruft Resolver-Ressourcen ab.
- `route53resolver:List*` – Hier können Sie eine Liste der Resolver-Ressourcen anzeigen.
- `ec2:DescribeNetworkInterfaces` – Hiermit können Sie eine Liste der Netzwerkschnittstellen anzeigen.
- `ec2:DescribeSecurityGroups` – Ermöglicht Ihnen das Anzeigen einer Liste mit all Ihren Sicherheitsgruppen.

Weitere Hinweise zu den Berechtigungen finden Sie unterAmazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "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 an eine servicegebundene Rolle angehängt, die es Route 53 Resolver ermöglicht, auf AWS -Services und Ressourcen zuzugreifen, die von 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 Amazon Route 53 53-Profilressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ec2`— Ermöglicht Principals, Informationen über VPCs abzurufen.

Weitere Informationen zu den Berechtigungen finden Sie unter. Amazon-Route-53-API-Berechtigungen: Referenztabelle für Aktionen, Ressourcen und Bedingungen

```
{
    "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:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

53-Updates an AWS verwaltete Richtlinien weiterleiten

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.

Änderung	Beschreibung	Datum
AmazonRoute53 ProfilesFullAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf Amazon Route 53 53-Profilressourcen zu ermöglichen.	22. April 2024
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 Route 53 Resolver ermöglicht, auf AWS Dienste und Ressourcen zuzugreifen, die von Resolver verwendet oder verwaltet werden.	14. Juli 2021
AmazonRoute53 ResolverReadOnlyAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, die den schreibgeschützten Zugriff auf Route 53-Resolver-Ressourcen ermöglicht.	14. Juli 2021
AmazonRoute53 ResolverFullAccess — Neue Richtlinie	Amazon Route 53 hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf Route 53 Resolver-Ressourcen zu ermöglichen.	14. Juli 2021

Änderung	Beschreibung	Datum
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
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, die den schreibgeschützten Zugriff auf Route 53-Ressourcen ermöglicht.	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 begann, Änderungen für seine AWS verwalteten Richtlinien nachzuverfolgen.	14. Juli 2021

Verwenden von IAM-Richtlinienbedingungen für die differenzierte Zugriffskontrolle zum Verwalten von Ressourcendatensätzen

Wenn Sie Berechtigungen für Ressourcendatensätze in Route 53 gewähren, können Sie Bedingungen angeben, die bestimmen, wie eine Berechtigungsrichtlinie wirksam wird.

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.
- Erteilen Sie Berechtigungen, damit Benutzer nur einen Teil der `CREATE | UPSERT | DELETE` Aktionen auf der Route 53-Konsole oder bei Verwendung der ChangeResourceRecordSetsAPI ausführen können.

Sie können auch Berechtigungen erstellen, die eine der detaillierten Berechtigungen kombinieren.

Verwenden Sie das IAM-`Condition`-Element, um eine differenzierte Zugriffskontrollrichtlinie zu implementieren. Indem ein `Condition`-Element einer Berechtigungsrichtlinie hinzugefügt wird, können Sie den Zugriff auf Datensätze in Route 53-Ressourceneintragssätzen, basierend auf Ihren Geschäftsanforderungen, ermöglichen oder verweigern. Beispielsweise kann Ihre IAM-Richtlinie den Zugriff auf einzelne DNS-Einträge in einer gehosteten Zone einschränken. Anschließend wenden Sie die Richtlinie auf Benutzer, Gruppen oder Rollen an.

Normalisieren der Bedingungsschlüsselwerte

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.

> **Important**
>
> Damit Ihre Berechtigungen Aktionen wie gewünscht zulassen oder einschränken können, müssen Sie diese Konventionen befolgen.

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 eine Reihe vordefinierter Bedingungsschlüssel (allgemeine 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.

Die folgende Tabelle zeigt die Route 53-Service-spezifischen Bedingungsschlüssel, die für Ressourcendatensätze gültig sind.

Route 53-Bedingungsschlüssel	API-Operationen	Werttyp	Beschreibung
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	Mehrwertig	Stellt eine Liste von DNS-Eintragsnamen in der Anfrage von dar. ChangeResource RecordSets 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.
`route53:ChangeReso`		Mehrwertig	Stellt eine Liste von Aktionen in der Anforderung von `ChangeResourceRecordSets` dar.

Route 53-Bedingungsschlüssel	API-Operationen	Werttyp	Beschreibung
`urceRecordSetsActions`	ChangeResourceRecordSets		`ChangeResourceRecordSetsActions` kann jeder der folgenden Werte sein (muss in Großbuchstaben sein): • CREATE • UPSERT • DELETE

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.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "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.

```
{
    "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.

```
{
    "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.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
```

```
}
```

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 mit Aktionen, Ressourcen und Bedingungsschlüsseln für Route 53, Aktionen, Ressourcen und Bedingungsschlüsseln für Route 53-Domänen, Aktionen, Ressourcen und Bedingungsschlüssel für Route 53 Resolver und Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Route 53-Profile verwenden, sodass DNS-Einstellungen mit VPCs in der Service Authorization Reference geteilt werden können. 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 mit anderen AWS-Services für weitere Protokollierungs- und Überwachungsmöglichkeiten integrieren.

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 Domäne oder Subdomäne, 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.

Verwenden von AWS CloudTrail zur Protokollierung von Konsolen und programmatischen Aktionen

CloudTrail bietet eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service in Route 53 durchgeführten Aktionen. Mithilfe der von CloudTrail gesammelten Informationen können Sie die Anfragen nachverfolgen, die ausgeführt wurden, sowie die IP-Adressen, von denen die Anforderungen stammen, den Initiator der Anfrage, den Zeitpunkt der Anfrage und weitere Details. Weitere Informationen finden Sie unter Protokollieren von Amazon Route 53-API-Aufrufen mit AWS CloudTrail.

Überwachung von Domänenregistrierungen

Das Route-53-Dashboard liefert detaillierte Informationen über den Status Ihrer Domänenregistrierungen, wie z. B. den Status von Domänenübertragungen und Domänen, die kurz vor dem Ablaufdatum stehen.

Weitere Informationen finden Sie unter Überwachung von Domainregistrierungen.

Verwenden von Route-53-Zustandsprüfungen und Amazon CloudWatch zur Überwachung Ihrer Ressourcen

Sie können Ihre Ressourcen mit Route-53-Zustandsprüfungen überwachen. Dabei werden Rohdaten von CloudWatch gesammelt und zu lesbaren Beinahe-Echtzeitmetriken verarbeitet.

Weitere Informationen finden Sie unter Überwachen Sie Ihre Ressourcen mit Amazon Route 53 Health Checks und Amazon CloudWatch.

Verwenden von Amazon CloudWatch zum Überwachen von Route-53-Resolver-Endpunkten

Sie können CloudWatch verwenden, um die Anzahl der DNS-Abfragen überwachen, die von Resolver-Endpunkten weitergeleitet werden.

Weitere Informationen finden Sie unter Überwachung von Route 53 Resolver-Endpunkten mit Amazon CloudWatch.

Verwenden von AWS Trusted Advisor

Trusted Advisor stützt sich auf bewährte Methoden auf der Grundlage langjähriger Services für AWS-Kunden. Trusted Advisor überprüft Ihre AWS-Umgebung und gibt dann Empfehlungen, sobald sich Möglichkeiten ergeben, Kosten zu senken, die Systemleistung zu verbessern oder Sicherheitslücken zu schließen. Alle AWS-Kunden haben Zugriff auf fünf Trusted Advisor-Überprüfungen. Kunden mit dem „Business“- oder „Enterprise“-Support-Plan können alle Trusted Advisor-Überprüfungen anzeigen.

Weitere Informationen finden Sie unter Trusted Advisor.

Compliance-Validierung für Amazon Route 53

Externe Prüfer bewerten im Rahmen verschiedener AWS-Compliance-Programme die Sicherheit und Compliance von Amazon Route 53. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie auf der Seite AWS-Services in Scope nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit AWS Artifact herunterladen. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

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 Gegenstand der Einhaltung von Standards wie HIPAA, PCI oder FedRAMP ist, stellt AWS Ressourcen zur Unterstützung bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientierten Basisumgebungen in 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-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort interessant sein.
- AWS Config – Dieser AWS-Service bewertet, zu welchem Grad die Konfiguration Ihrer Ressourcen den internen Vorgehensweisen, Branchenrichtlinien und Vorschriften entspricht.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit in Amazon Route 53

Im Zentrum der globalen AWS Infrastruktur stehen die AWS-Regionen und Availability Zones (Verfügbarkeitszonen, AZs). AWS Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die mit Netzwerken mit geringer Latenz, hohem Durchsatz und hochredundanten Vernetzungen 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 Service, aber die folgenden Funktionen unterstützen AWS-Regionen:

- Wenn Sie Route 53 Resolver zum Einrichten von Hybrid-Konfigurationen verwenden, erstellen Sie Endpunkte in AWS-Regionen, die Sie auswählen, und geben Sie IP-Adressen in mehreren Availability Zones. 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? Amazon Route 53 Resolver.
- Sie können Route-53-Zustandsprüfungen konfigurieren, um den Zustand der Ressourcen, die Sie erstellen, in bestimmten Regionen zu prüfen, z. B. Amazon-EC2-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 über AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in Amazon Route 53

Als verwalteter Service ist Amazon Route 53 durch die globale Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch 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.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

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:

- Die angeforderte Domain oder Subdomain

- Das Datum und die Uhrzeit der Anforderung
- DNS-Datensatztyp (z. B. A oder AAAA)
- Der Route 53-Edge-Standort, 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 Protokolle an CloudWatch Logs. Sie verwenden CloudWatch Logs-Tools, um auf die Abfrageprotokolle zuzugreifen.

Abfrageprotokolle enthalten nur die Abfragen, die DNS-Auflöser 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 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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.

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 der einzelnen Protokoll-Streams ist *`hosted-zone-id`*/*`edge-location-ID`*, z. B. `Z1D633PJN98FT9/DFW3`.

Jeder Edge-Standort wird anhand eines Codes aus drei Buchstaben und einer willkürlich zugewiesenen 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 Route 53-Konsole unter https://console.aws.amazon.com/route53/ an AWS Management Console und öffnen Sie sie.

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. Jeder Edge-Standort wird anhand eines Codes aus drei Buchstaben und einer willkürlich zugewiesenen 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.

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 von Ihnen angegebenen Amazon Virtual Private Cloud VPCs stammen, 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 Route 53 Resolver-DNS-Firewall-Regeln verwenden, um Domainlisten zu blockieren, zu erlauben oder zu überwachen.

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 in DNS-Abfrageprotokollenaus.

> **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-Resolver speichert Abfragen, die aus Ihren VPCs stammen, und reagiert nach Möglichkeit

aus dem Cache, um Antworten zu beschleunigen. Die Protokollierung der Resolver-Abfrage protokolliert nur eindeutige Abfragen, nicht Abfragen, auf die Resolver aus dem Cache antworten kann.
Angenommen, eine EC2-Instance in einer der VPCs, für die eine Abfrageprotokollierungskonfiguration Abfragen protokolliert, sendet eine Anforderung für accounting.example.com. Resolver speichert die Antwort auf diese Abfrage und protokolliert die Abfrage. Wenn die elastische Netzwerkschnittstelle der gleichen Instance eine Abfrage für accounting.example.com innerhalb der TTL des Cache des Resolver vornimmt, antwortet 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 Resolver-Abfrageprotokolle senden können.

Themen

AWS Ressourcen, an die Sie 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 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 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:

```
{
    "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 Resolver-Protokollen fallen Protokollgebühren an, auch wenn Protokolle direkt in Amazon S3 veröffentlicht werden. Weitere Informationen finden Sie unter Versandprotokolle an S3 zu CloudWatch Amazon-Preisen.

Konfigurationen für die Protokollierung von Resolver-Abfragen verwalten

Konfigurieren (Protokollierung der Resolver-Abfrage)

Um die Protokollierung von DNS-Abfragen zu starten, die von Ihren VPCs stammen, führen Sie die folgenden Aufgaben in der Amazon Route 53-Konsole aus:

So konfigurieren Sie die Protokollierung der Resolver-Abfrage

1. Melden Sie sich unter https://console.aws.amazon.com/route53/ bei der Route 53-Konsole an AWS Management Console und öffnen Sie sie.
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. Dabei muss es sich um dieselbe Region handeln, in der Sie die VPCs erstellt haben, für die Sie DNS-Abfragen protokollieren möchten. Wenn Sie VPCs in mehreren Regionen haben, müssen Sie für jede Region mindestens eine Konfiguration für die Abfrageprotokollierung 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 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 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 Konfiguration für die

Abfrageprotokollierung erstellen. Wenn Sie eine neue Ressource erstellen, wird diese Ressource in derselben Region erstellt.

VPCs zum Protokollieren von Abfragen

Diese Konfiguration für die Abfrageprotokollierung protokolliert DNS-Abfragen, die aus den ausgewählten VPCs stammen. Aktivieren Sie das Kontrollkästchen für jede VPC in der aktuellen Region, für die Resolver Abfragen protokollieren soll, und wählen Sie Auswählen 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 aus.

> **Note**
>
> Nach dem erfolgreichen Erstellen der Konfiguration für die Abfrageprotokollierung sollten Sie die DNS-Abfragen in Ihrer VPC in den Protokollen anzeigen.

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:

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 Resolver als Antwort auf die DNS-Abfrage 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 der möglichen Antwortcodes finden Sie unter DNS RCODES auf der IANA-Website.

Antwort_Typ

Der DNS-Datensatztyp (z. B. A, MX oder CNAME) des Werts, den Resolver als Antwort auf die Abfrage zurückgibt. Informationen zu den von Route 53 unterstützten Typen finden Sie unter Unterstützte DNS-Datensatztypen.

rdata

Der DNS-Antwortcode, den Resolver als Antwort auf die DNS-Abfrage zurückgegeben hat. Bei einem A-Datensatz handelt es sich hierbei beispielsweise um eine IP-Adresse im IPv4-Format. Für einen CNAME-Datensatz ist dies der Domainname im CNAME-Datensatz.

Antwort_Klasse

Die Klasse der Resolver-Antwort auf die Abfrage.

srcaddr

Die IP-Adresse der Instance, von der die Abfrage stammt.

srcport

Der Port auf der Instance, von der die Abfrage stammt.

Transport

Das Protokoll, das zum Senden der DNS-Abfrage verwendet wird.

srcids

Die IDs der `instance`, des `resolver_endpoint` und der `resolver_network_interface`, von denen die DNS-Abfrage stammt oder durch die sie übergeben wurde.

Instance

Die ID der Instance, von der die Abfrage stammt.

resolver_endpoint

Die ID des Auflösungsendpunkts, der die DNS-Abfrage an On-Premises-DNS-Server weiterleitet.

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 Resolver

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"
    }
```


Resolver-Konfigurationen für die 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 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 von VPCs mit Konfigurationen für gemeinsame Abfrageprotokollierung

Wenn ein anderes AWS Konto eine oder mehrere Konfigurationen mit Ihrem Konto gemeinsam genutzt hat, können Sie VPCs der Konfiguration genauso zuordnen, wie Sie VPCs Konfigurationen zuordnen, die Sie erstellt haben.

Löschen oder Aufheben der Freigabe einer Konfiguration

Wenn Sie eine Konfiguration für andere Konten freigeben und die Konfiguration dann entweder löschen oder die Freigabe aufheben, die Konfiguration jedoch mit einer oder mehreren VPCs verknüpft waren, stoppt Route 53 Resolver die Protokollierung von DNS-Abfragen, die aus diesen VPCs stammen.

Maximale Anzahl der Konfigurationen für die Abfrageprotokollierung und VPCs, die einer Konfiguration zugeordnet werden können

Wenn ein Konto eine Konfiguration erstellt und für ein oder mehrere andere Konten freigibt, gilt der Höchstwert für die Anzahl an VPCs, die der Konfiguration zugeordnet werden können,

pro Konto. 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 ordnen die Konfiguration dann ihren VPCs zu und zählen sie anhand der VPC-Zuordnungen der Abfrageprotokollkonfiguration ihres Kontos pro Limit von 100 pro AWS-Region . Wenn sich jedoch alle VPCs in einem einzigen Konto befinden, müssen die Service-Limits des Kontos möglicherweise erhöht werden.

Aktuelle Resolver-Kontingente finden Sie unter Kontingente bei Route 53 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 Route 53-Konsole an AWS Management Console und öffnen Sie sie 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 Seite Rule: ***rule name*** zeigt der Wert unter Owner (Eigentümer) die ID des Kontos an, das die Regel erstellt hat. 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 Konfiguration für die Abfrageprotokollierung mit einem anderen AWS Konto, einer anderen Organisationseinheit oder Organisation gemeinsam zu verwenden, 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.

Beschreibung

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.

Auftraggeber

Geben Sie die AWS Kontonummer, den Namen der Organisationseinheit oder den Namen der Organisation ein.

Tags

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 Billing and Cost Management 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.

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

Der Namespace `AWS/Route53` enthält die folgenden Metriken zu Route 53-Zustandsprüfungen.

ChildHealthCheckHealthyZählen

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

SSL HandshakeTime

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 es weglassen`Region`, werden Metriken 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 unter GetMetricStatistiken in 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.

DNSSEC InternalFailure

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.

DNSSEC-Aktion KeySigning KeysNeeding

Anzahl der Schlüsselsignierungsschlüssel (KSKs), die den Status ACTION_NEEDED (aufgrund eines KMS-Fehlers) aufweisen.

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.

DNSSEC Alter KeySigning KeyMax NeedingAction

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.

DNSSEC KeySigning KeyAge

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 Resolver-Endpunkten mit Amazon CloudWatch

Sie können Amazon verwenden CloudWatch , um die Anzahl der DNS-Abfragen zu überwachen, die von Route 53 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 vorsignierten URLs finden Sie unter Was ist? Amazon Route 53 Resolver. Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Metriken und Dimensionen für Route 53 Resolver

Wenn Sie Resolver so konfigurieren, dass DNS-Anfragen an Ihr Netzwerk weitergeleitet werden oder umgekehrt, sendet Resolver alle fünf Minuten Metriken und Dimensionen, und zwar CloudWatch ungefähr so viele Anfragen, die weitergeleitet werden. 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 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 mit dem aktuellen Konto erstellt wurden. AWS Wählen Sie dann InboundQueryVolume oder Volume, um die gewünschten OutboundQueryZählungen anzuzeigen.

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 Route 53 Resolver
- Dimensionen für Route 53 Resolver

CloudWatch Metriken für Route 53 Resolver

`AWS/Route53Resolver`-Namespace enthält Metriken für Route 53-Endpunkte und für IP-Adressen.

Themen

- Metriken für Resolver-Endpunkte
- Metriken für Resolver-IP-Adressen

Metriken für Resolver-Endpunkte

Der `AWS/Route53Resolver`-Namespace enthält die folgenden Metriken für Route 53 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, Summe, Durchschnitt

Einheiten: Anzahl

EndpointUnhealthyEni zählen

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, Summe, Durchschnitt

Einheiten: Anzahl

InboundQueryVolumen

Für eingehende Endpunkte wird die Anzahl der DNS-Abfragen, die von Ihrem Netzwerk an Ihre VPCs über den Endpunkt weitergeleitet werden, durch `EndpointId` angegeben.

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryVolumen

Für ausgehende Endpunkte wird die Anzahl der DNS-Abfragen, die von Ihrer VPC an Ihr Netzwerk über den Endpunkt weitergeleitet werden, durch `EndpointId` angegeben.

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryAggregateVolume

Bei ausgehenden Endpunkten die Gesamtzahl der DNS-Abfragen, die von Amazon VPCs an Ihr Netzwerk weitergeleitet werden, einschließlich der folgenden:

- Die Anzahl der DNS-Abfragen, die von Ihren VPCs über den durch `EndpointId` festgelegten Endpunkt an Ihr Netzwerk weitergeleitet werden.
- Wenn das aktuelle Konto Resolver-Regeln mit anderen Konten teilt, die Abfragen von VPCs, die von anderen Konten erstellt wurden, die über den Endpunkt, der durch die `EndpointId` angegeben wird, an Ihr Netzwerk weitergeleitet werden.

Gültige Statistiken: Summe

Einheiten: Anzahl

Metriken für 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 Resolver eine elastische Amazon VPC-Netzwerkschnittstelle.)

InboundQueryVolumen

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 ListResolver EndpointIp Adressen abrufen.

Gültige Statistiken: Summe

Einheiten: Anzahl

OutboundQueryAggregateVolume

Für jede IP-Adresse für Ihre ausgehenden Endpunkte die Gesamtzahl der DNS-Abfragen, die von Amazon VPCs an Ihr Netzwerk weitergeleitet werden, einschließlich der folgenden:

- Die Anzahl der DNS-Abfragen, die von Ihren VPCs unter Verwendung der angegebenen IP-Adresse an Ihr Netzwerk weitergeleitet werden.
- Wenn das aktuelle Konto Resolver-Regeln mit anderen Konten teilt, die Abfragen von VPCs, die von anderen Konten erstellt werden, die unter Verwendung der angegebenen 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 Addresses abrufen. ListResolver EndpointIp

Gültige Statistiken: Summe

Einheiten: Anzahl

Dimensionen für Route 53 Resolver

Route 53-Metriken für ein- und ausgehende Endpunkte verwenden den Namespace `AWS/Route53Resolver` und stellen Metriken für `EndpointId` bereit. 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.

Die Dimension `RniId` wird für Metriken vom Typ `OutboundQueryAggregateVolume` und `InboundQueryVolume` unterstützt.

Überwachung von Route 53 Resolver DNS-Firewall-Regelgruppen mit Amazon CloudWatch

Sie können Amazon verwenden CloudWatch , um die Anzahl der DNS-Abfragen zu überwachen, die von Route 53 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 Route 53 Resolver DNS Firewall. Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

Metriken und Dimensionen für Route 53 Resolver DNS Firewall

Wenn Sie einer VPC eine Route 53 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 die Route 53 Resolver DNS Firewall.

Sie können die folgenden Verfahren verwenden, um die Metriken in der CloudWatch Konsole anzuzeigen, oder sie mithilfe von AWS Command Line Interface ()AWS CLI anzeigen.

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 All metrics (Alle Metriken) die Option Route 53 Resolver.
5. Wählen Sie eine Metrik aus, die Sie interessieren.

Um Metriken mit dem anzuzeigen AWS CLI

- Geben Sie in einer Eingabeaufforderung den folgenden Befehl ein:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Themen

- CloudWatch Metriken für die Route 53 Resolver DNS Firewall

CloudWatch Metriken für die Route 53 Resolver DNS Firewall

Der `AWS/Route53Resolver`-Namespace enthält Metriken für Regelgruppen von Route 53 Resolver DNS Firewall.

Themen

Metriken für Route 53 Resolver DNS Firewall

FirewallRuleGroupQueryVolumen

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`

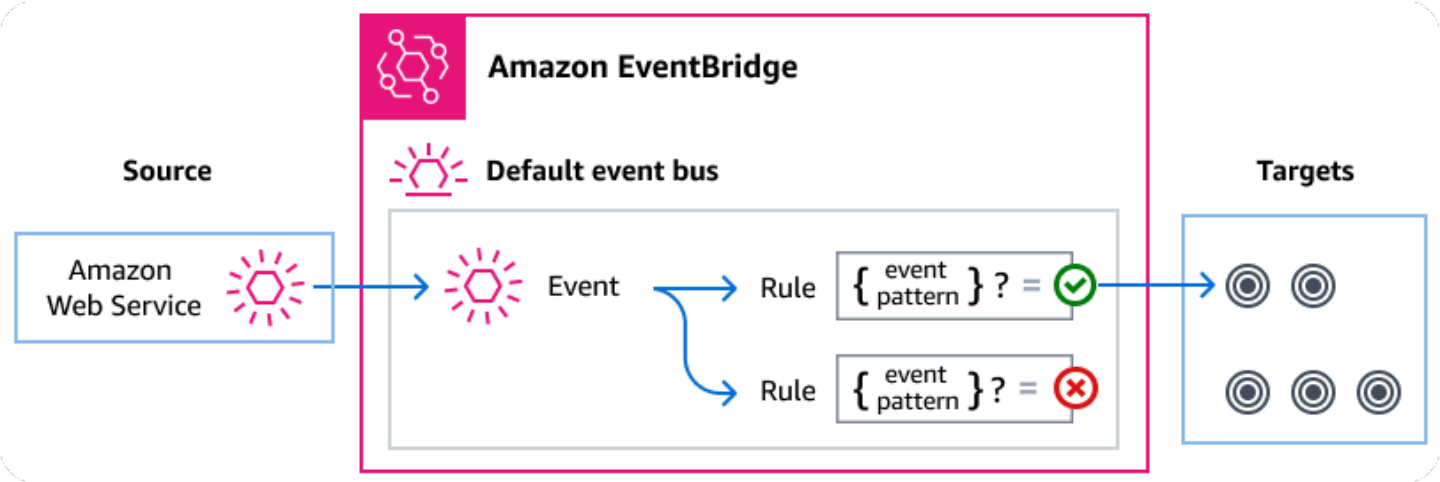
Gültige Statistiken: Summe

Einheiten: Anzahl

Verwaltung von Route 53 Resolver-DNS-Firewallereignissen 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 Änderung in einer Ressource oder Umgebung dar.

Wie bei vielen AWS Diensten generiert die DNS-Firewall Ereignisse und sendet sie an den EventBridge Standardereignisbus. (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. Regeln, die Sie für den Event-Bus angeben, werten Ereignisse aus, sobald sie eintreffen. Jede Regel prüft, ob ein Ereignis dem Ereignismuster der Regel entspricht. Wenn das Ereignis übereinstimmt, sendet der Event-Bus das Ereignis an die angegebenen Ziele.



Themen

Route 53 Resolver DNS-Firewall-Ereignisse

Route 53 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. .

Art der Einzelheiten des Ereignisses	Beschreibung
DNS-Firewall-Block	Jede Blockaktion, die auf einer Domain ausgeführt wird.
DNS-Firewall-Warnung	Jede Warnungsaktion, die auf einer Domain ausgeführt wurde.

Senden von Route 53 Resolver DNS-Firewallereignissen 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:
   - Route 53 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.

Erstellen von Ereignismustern für Route 53 Resolver DNS-Firewallereignisse

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. Beispielsweise:

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 T1+30 Minuten eine DNS-Abfrage 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 mit den gewünschten Ereignissen übereinstimmt. 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.

Für die von Ihnen angegebenen Ziele sind möglicherweise bestimmte Berechtigungen oder Konfigurationen erforderlich. 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 für EventBridge den Abgleich von Ereignissen mit Regeln 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 Route-53-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",
      "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.

`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-Alarmereignis

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",
 "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

Im Folgenden finden Sie die Detailfelder für den *Ereignisnamen*.

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",
      "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.

`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",
 "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 die Route 53-APIs. 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

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 im CloudTrail Ereignisverlauf 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 standardmäßig 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 hier:

- 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. Beispielsweise generieren Aufrufe der `RegisterDomain` Aktionen `CreateHostedZoneCreateHealthCheck`, und 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 dem CloudTrail UserIdentity-Element.

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 eines ausgehenden Endpunkts für Route 53 Resolver


```
{
    "Records": [
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
            "eventName": "ListHostedZones",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2015-01-16T00:41:48Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": null,
            "responseElements": null,
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
```

```
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
            "eventName": "CreateHealthCheck",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:57Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "callerReference": "2014-05-06 64832",
                "healthCheckConfig": {
                    "iPAddress": "192.0.2.249",
                    "port": 80,
                    "type": "TCP"
                }
            },
            "responseElements": {
                "healthCheck": {
                    "callerReference": "2014-05-06 64847",
                    "healthCheckConfig": {
                        "failureThreshold": 3,
                        "iPAddress": "192.0.2.249",
                        "port": 80,
                        "requestInterval": 30,
                        "type": "TCP"
                    },
                    "healthCheckVersion": 1,
                    "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
                },
                "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
```

```
            }
        },
        {
            "additionalEventData": {
                "Note": "Do not use to reconstruct hosted zone"
            },
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
            "eventName": "ChangeResourceRecordSets",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:43Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "changeBatch": {
                    "changes": [
                        {
                            "action": "CREATE",
                            "resourceRecordSet": {
                                "name": "prod.example.com.",
                                "resourceRecords": [
                                    {
                                        "value": "192.0.1.1"
                                    },
                                    {
                                        "value": "192.0.1.2"
                                    },
                                    {
                                        "value": "192.0.1.3"
                                    },
                                    {
                                        "value": "192.0.1.4"
                                    }
                                ],
                                "tTL": 300,
                                "type": "A"
                            }
                        },
                        {
                            "action": "CREATE",
                            "resourceRecordSet": {
```

```
                            "name": "test.example.com.",
                            "resourceRecords": [
                                {
                                    "value": "192.0.1.1"
                                },
                                {
                                    "value": "192.0.1.2"
                                },
                                {
                                    "value": "192.0.1.3"
                                },
                                {
                                    "value": "192.0.1.4"
                                }
                            ],
                            "tTL": 300,
                            "type": "A"
                        }
                    }
                ],
                "comment": "Adding subdomains"
            },
            "hostedZoneId": "Z1PA6795UKMFR9"
        },
        "responseElements": {
            "changeInfo": {
                "comment": "Adding subdomains",
                "id": "/change/C156SRE0X2ZB10",
                "status": "PENDING",
                "submittedAt": "Jan 16, 2018 12:41:43 AM"
            }
        },
        "sourceIPAddress": "192.0.2.92",
        "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
        "userIdentity": {
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "accountId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "type": "IAMUser",
            "userName": "smithj"
        }
    },
    {
```

```
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "0cb87544-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

Die Themen in diesem Kapitel helfen Ihnen bei der Behebung von Problemen mit Ihrer Domänenregistrierung und DNS-Konfiguration.

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-Service für die Domain verwenden, melden Sie sich bei der an AWS Management Console 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-Service für die Domain verwenden, melden Sie sich bei der an AWS Management Console 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 Sperrung 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 AWS zum ersten Mal bei registrieren, verlangt ICANN, dass wir eine Bestätigung erhalten, dass die E-Mail-Adresse für den Registrierenden-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.

> **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 für Betrug gesperrt ist.)

Um eine Sperrung anzufechten, senden Sie eine E-Mail an abuse@amazon.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 einen Gerichtsbeschluss anzufechten, senden Sie eine E-Mail an abuse@amazon.com und fügen Sie die relevanten Dokumente an.

Übertragen meiner Domäne an Amazon Route 53 fehlgeschlagen

Hier finden Sie häufige Gründe für das Fehlschlagen der Übertragung einer Domain in Amazon 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) als Punycode, der Unicode-Zeichen als ASCII-Zeichenfolgen darstellt.

Wenn beim Übertragen eines IDNs auf Route 53 eine Fehlermeldung angezeigt wird, stellen Sie ihn mit Punycode dar und versuchen Sie es erneut. Weitere Informationen finden Sie unter Formatierung internationalisierter Domänennamen.

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.
- Sie haben den DNS-Dienst kürzlich an Amazon Route 53 übertragen, die Namenserver bei der Domainvergabestelle aber nicht aktualisiert.

- DNS-Resolver verwenden immer noch die alten Einstellungen für den Datensatz.
- Sie haben mehr als eine gehostete Zone mit demselben Namen, und Sie haben diejenige aktualisiert, die nicht mit der Domäne verknüpft ist

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 Management Console 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 Alias-Datensätzen wird die TTL durch die AWS Ressource bestimmt, an die der Datensatz Datenverkehr 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 Management Console 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.

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 einfach, den falschen Wert anzugeben, z. B. die IP-Adresse für einen Webserver oder den Domänennamen, der Ihrer Webverteilung CloudFront 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 den Datenverkehr an einen S3-Bucket weiterleiten möchten, der für das Website-Hosting konfiguriert ist, der Name des Buckets jedoch nicht in der Alias-Zielliste in der Amazon-Route-53-Konsole angezeigt wird, oder wenn Sie versuchen, einen Aliasdatensatz programmgesteuert zu erstellen, und Sie eine InvalidInput Fehlermeldung von der Route-53-API, einem der - AWS SDKs AWS CLI, der oder erhalten AWS Tools for Windows PowerShell, überprüfen Sie 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 in Rechnung gestellt

Wenn Sie sich für ein Abonnement anmelden, eine Registrierungsgebühr, eine Übertragungsgebühr oder eine Verlängerungsgebühr mit Vorauszahlung bezahlen, wird eine eindeutige Rechnung

generiert. Diese Rechnung verbleibt in der Fakturierungskonsole, auch wenn die Zahlungstransaktion nicht erfolgreich ist. Der zugehörige Fakturierungsposten wird als [x]-Menge im Unterbereich Registrar-Global der Registerkarte Rechnungsdetails nach Service in der Fakturierungskonsole angezeigt.

Führen Sie die folgenden Schritte aus, um die abgelehnten Rechnungen anzuzeigen:

So zeigen Sie die abgelehnten Rechnungen in der Fakturierungskonsole an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - AWS Billing Konsole unter https://console.aws.amazon.com/billing/.
2. Wählen Sie im Navigationsbereich Rechnungen aus.
3. Wählen Sie Rechnungen, um Details zu allen abgelehnten Rechnungen anzuzeigen.

Führen Sie die folgenden Schritte aus, um die erfolgreichen Zahlungen und Erstattungen in der Fakturierungskonsole anzuzeigen:

So bestätigen Sie die Zahlungen oder Erstattungen, 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 anzuzeigen AWS.

Mein AWS Konto ist geschlossen, gesperrt oder aufgelöst und meine Domain ist bei Route 53 registriert

Wenn Sie Ihr AWS Konto geschlossen haben oder das Konto gesperrt oder aufgelöst ist und die automatische Verlängerung aktiviert ist, versucht Route 53, die Domänenregistrierung zu verlängern, aber die Verlängerungen schlagen fehl. Sie können sich an den - AWS Support wenden und ihn um Hilfe bei den folgenden Optionen bitten:

- Wenn Sie die Domänenregistrierung nicht beibehalten möchten, kann AWS Support die automatische Verlängerung für die Domäne deaktivieren. Dies verhindert, dass Sie mehrere Erinnerungs-E-Mails zur Domänenverlängerung erhalten.
- Wenn Sie die Domänenregistrierung beibehalten möchten, kann AWS Ihnen Support dabei helfen, entweder Ihr Konto zu reaktivieren oder die Domäne an eine andere Domänenvergabestelle zu übertragen.

> **Note**
>
> Sobald 90 Tage seit der Schließung Ihres Kontos vergangen sind, können Sie es nicht mehr erneut öffnen. Weitere Informationen finden Sie unter Kann ich mein geschlossenes wieder öffnen AWS-Konto?.

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**
>
> Wir ändern die IP-Adressen von Namensservern selten. Wenn wir die IP-Adressen ändern müssen, benachrichtigen wir Sie im Voraus.

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 selten die IP-Adressbereiche von Zustandsprüfungen. Wenn wir IP-Adressbereiche ändern müssen, werden wir Sie im Voraus benachrichtigen.

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 Amazon-EC2-Instance müssen eingehenden Datenverkehr von den IP-Adressen zulassen, die von den Route-53-Zustandsprüfungen verwendet werden. Ein Verweis auf eine Präfixliste vereinfacht die Verwaltung der CIDR-Blöcke in Ihren Regeln. Wenn Sie häufig die gleichen CIDRs in mehreren Regeln verwenden, können Sie diese CIDRs in einer einzelnen Präfixliste verwalten, anstatt in jeder Regel immer wieder auf die gleichen CIDRs 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 Von verwaltete Präfixlisten sind Gruppen von IP-Adressbereichen für AWS- AWS Services. Von verwaltete Präfixlisten werden von erstellt und verwaltet AWS und können von jedem mit einem - AWS Konto verwendet werden. Sie können eine von AWS verwaltete Präfixliste nicht erstellen, ändern, freigeben oder löschen.

Weitere Informationen zu von AWS verwalteten Präfixlisten finden Sie unter Arbeiten mit von verwalteten Präfixlisten im Amazon AWS-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 (Markierung) ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jedes Tag besteht aus einem Schlüssel und einem Wert, die Sie beide selbst definieren. Der Schlüssel könnte beispielsweise „domain“ heißen und der Wert „example.com“. Sie können Tags für verschiedene Zwecke nutzen; eine häufige Nutzung ist die Kategorisierung und Nachverfolgung der Amazon-Route-53-Kosten. Wenn Sie Tags auf gehostete Route-53-Zonen, Domänen und Zustandsprüfungen anwenden, generiert AWS einen Kostenzuordnungsbericht als CSV-Datei mit Ihrer Nutzung und Kosten gemäß Ihren Tags. 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.

Der Tag (Markierung)-Editor in der AWS Management Console ist benutzerfreundlich und am besten dazu geeignet, Tags (Markierungen) zentral und einheitlich zu erstellen und zu verwalten. Weitere Informationen finden Sie unter Arbeiten mit dem Tag Editor in Erste Schritte mit der AWS Management Console. 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-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**
>
> Gebühren für Resolver beruhen teilweise auf VPC-Elastic-Network-Schnittstellen, die mit den IP-Adressen übereinstimmen, die Sie für eingehende und ausgehende Endpunkte festlegen. Sie können derzeit keine Elastic-Network-Schnittstellen bezeichnen, die von Resolver erstellt werden, sodass Sie keine Tags für die Zuweisung von die Kosten für Resolver verwenden

können. Weitere Informationen zu Preisen für 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 den folgenden Tutorials wird erläutert, wie Sie Aamzon Route 53 als DNS-Service für eine Subdomäne nutzen, während Sie gleichzeitig einen anderen DNS-Service für die Domäne verwenden. Außerdem wird erläutert, wie Sie für verschiedene Anwendungsfälle in Verbindung mit gewichteten und Latenz-Datensätzen einsetzen können.

Themen

Verwendung von Amazon Route 53 als DNS-Service für eine Subdomäne ohne Migration der übergeordneten Domäne

Sie können Amazon Route 53 als DNS-Service für eine neue Subdomäne oder eine vorhandene Subdomäne verwenden und weiterhin einen anderen DNS-Service für die übergeordnete Domäne nutzen. Weitere Informationen finden Sie im entsprechenden Thema.

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 ist die einzige Möglichkeit, zu überprüfen, ob die Änderungen weitergegeben wurden, die Verwendung der API-Aktion GetChange. 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 bereits Route 53 als DNS-Dienst für Ihre Domäne verwenden und den Datenverkehr für eine Subdomäne (z. B. www.example.com) an ihre Ressourcen weiterleiten möchten, beispielsweise an einen Webserver, der auf einer EC2-Instance ausgeführt wird, informieren Sie sich 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 unter ChangeResourceRecordSets in 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 ChangeResourceRecordSets zum Erstellen Ihrer Datensätze verwendet haben, können Sie die `GetChange` -Aktion verwenden, um zu bestimmen, ob Ihre Änderungen weitergegeben wurden. (`ChangeResourceRecordSets` gibt einen Wert für `ChangeId` zurück, den Sie in eine nachfolgende `GetChange`-Anforderung aufnehmen können. `ChangeId` ist nicht verfügbar, wenn Sie die Datensätze mithilfe 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-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 AWS Management Console-Managementkonsole an 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 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 unter GetHostedZone in 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 ist die einzige Möglichkeit, zu überprüfen, ob die Änderungen weitergegeben wurden, die Verwendung der API-Aktion GetChange. Änderungen werden im Allgemeinen innerhalb von 60 Sekunden an alle Route-53-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 bereits Route 53 als DNS-Dienst für Ihre Domäne verwenden und den Datenverkehr für eine Subdomäne (z. B. www.example.com) an ihre Ressourcen weiterleiten möchten, beispielsweise an einen Webserver, der auf einer EC2-Instance ausgeführt wird, informieren Sie sich 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 Datenverkehr für Ihre Domänen und Subdomänen weitergeleitet werden soll. Wenn beispielsweise jemand Ihren Domänennamen in einen Webbrowser eingibt, möchten Sie, dass der Datenverkehr an einen Webserver in Ihrem Rechenzentrum, an eine Amazon-EC2-Instance, an eine CloudFront-Verteilung oder an einen anderen Ort geleitet 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 unter ChangeResourceRecordSets in 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 ChangeResourceRecordSets zum Erstellen Ihrer Datensätze verwendet haben, können Sie die `GetChange` -Aktion verwenden, um zu bestimmen, ob Ihre Änderungen weitergegeben wurden. (`ChangeResourceRecordSets` gibt einen Wert für `ChangeId` zurück, den Sie in eine nachfolgende `GetChange`-Anforderung aufnehmen können. `ChangeId` ist nicht verfügbar, wenn Sie die Datensätze mithilfe 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-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 AWS Management Console-Managementkonsole an 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 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 unter GetHostedZone in 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 AWS-Endpunkt mit der niedrigsten Latenz weiterleiten. Sie können beispielsweise einen DNS-Namen wie `www.example.com` mit einem ELB Classic, Application oder Network Load Balancer oder mit Amazon-EC2-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**
>
> 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 einer AWS-Region 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. Nehmen wir ein Beispiel, in dem `www.example.com` aktuell auf einer Amazon-EC2-Instance in der Region USA Ost (Ohio) gehostet wird. Die Instance hat die Elastic IP-Adresse `W.W.W.W`. Nehmen wir an, dass Sie weiterhin Datenverkehr zur Region USA Ost (Ohio) leiten möchten (sofern zutreffend), Benutzer aber allmählich auch zu weiteren Amazon-EC2-Instances in der Region USA West (Nordkalifornien) (Elastic IP `X.X.X.X`) und der Region Europa (Irland) (Elastic IP `Y.Y.Y.Y`) leiten möchten. 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 wandeln Ihren vorhandenen Datensatz für `www.example.com` in einen gewichteten Aliasdatensatz um, der weiterhin den Großteil Ihres Datenverkehrs zu Ihrer bestehenden Amazon-EC2-Instance in der Region USA Ost (Ohio) leitet.
- 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 ausschließlichen Weiterleitung von Datenverkehr zur Region USA Ost (Ohio) zur Weiterleitung von Datenverkehr zu allen drei Regionen übergehen, in denen Sie über Amazon-EC2-Instances verfügen.

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 Latenz-Datensatz für jede Ihrer Amazon-EC2-Instances, z. B.:

   - 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 Latenz-Datensatz `www-lbr.example.com` zu dem gewichteten Datensatz `www.example.com` hinzu und beginnen wir mit der Weiterleitung einer begrenzten Menge an Datenverkehr an die entsprechenden Amazon-EC2-Instances. Dies bedeutet, dass die Amazon-EC2-Instance in der Region USA Ost (Ohio) Datenverkehr von beiden gewichteten Datensätzen erhalten wird.

   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 auf Route-53-Servern synchronisiert werden, beginnt Route 53 damit, einen sehr kleinen Teil Ihres Datenverkehr (1/101) an die Amazon-EC2-Instances zu leiten, für die Sie in Schritt 3 Latenz-Datensätze 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 Datenverkehr für `www.example.com` weiterzuleiten und möchten eine Amazon-EC2-Instance in der Region Asien-Pazifik (Tokio) zu

Ihren Instances in den Regionen USA Ost (Ohio), USA West (Nordkalifornien) und Europa (Irland) 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, beginnt Route 53 damit, einen sehr kleinen Teil Ihres Datenverkehrs (1/101) an die Amazon-EC2-Instances zu leiten, für die Sie in Schritt 1 die `www-lbr-2012-04-30.example.com`-Latenz-Datensätze erstellt haben. Der Rest des Datenverkehrs wird weiterhin an die `www-lbr.example.com`-Latenz-Datensätze geleitet, die nicht die Amazon-EC2-Instance in der Region Asien-Pazifik (Tokio) umfassen.
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.

Verwenden von Latenz- und gewichteten Datensätzen in Amazon Route 53, um Datenverkehr an mehrere Amazon-EC2-Instances in einer Region weiterzuleiten

Wenn Ihre Anwendung auf Amazon-EC2-Instances in zwei oder mehr Amazon-EC2-Regionen ausgeführt wird und Sie über mehr als eine Amazon-EC2-Instance in einer oder mehreren Regionen verfügen, können Sie latenzbasiertes Routing verwenden, um Datenverkehr an die richtige Region zu leiten, und anschließend Datenverkehr mittels gewichteter Datensätze basierend auf selbst festgelegten Gewichtungen an Instances innerhalb der Region leiten.

Angenommen, Sie haben drei Amazon-EC2-Instances mit Elastic-IP-Adressen in der Region USA Ost (Ohio) und Sie möchten Anfragen für Benutzer, für die die Region USA Ost (Ohio) die angemessene Region ist, gleichmäßig auf alle drei IPs aufteilen. Eine Amazon-EC2-Instance in

den anderen Regionen ist ausreichend, auch wenn Sie die gleiche Vorgehensweise für mehrere Regionen gleichzeitig anwenden können.

Verwenden von Latenz- und gewichteten Datensätzen in Amazon Route 53, um Datenverkehr an mehrere Amazon-EC2-Instances in einer Region weiterzuleiten

1. Erstellen Sie eine Gruppe von gewichteten Datensätzen für die Amazon-EC2-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 eine gleichmäßige Gewichtung der Amazon-EC2-Instances wünschen, geben Sie bei Gewicht denselben Wert 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 Amazon-EC2-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 einen Latenz-Aliasdatensatz für jede Region, in der Sie über mehrere Amazon-EC2-Instances verfügen (beispielsweise USA Ost (Ohio)). 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 einen Latenz-Datensatz für jede Region, in der Sie über eine Amazon-EC2-Instance verfügen. 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 Wert-/Route-Datenverkehr nach, IP-Adresse oder anderer Wert, abhängig vom Datensatztyp aus und geben Sie die Elastic-IP-Adresse der Amazon-EC2-Instance in dieser Region an.

   Weitere Information zum Hinzufügen von Aliasdatensätzen zu Amazon EC2 EC2-Instances finden Sie unter Weiterleiten des Datenverkehrs an eine Amazon-EC2-Instance

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.

Angenommen, Sie verfügen über acht Amazon-EC2-Instances oder Elastic-IP-Endpunkte für einen Service. 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 auch dem Ausfall einer Availability Zone vorbeugen, indem Sie Antworten konfigurieren, die eine Mischung von IPs enthalten, die in zwei oder mehr Availability Zones gehostet sind.

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

Folgen Sie diesen bewährten Methoden bei Ihrer Konfiguration von Route 53.

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 die Routenkontrolle von Amazon Route 53 Application Recovery Controller sind global verteilt und auf 100 % Verfügbarkeit und Funktionalität ausgelegt, auch bei schweren 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 Failover während der Notfallwiederherstellung empfehlen wir Ihnen, Funktionen wie Route-53-Zustandsprüfungen und Route-53-ARC-Routenkontrolle zu verwenden, die für das Aktualisieren von DNS auf die Funktionalität der Datenebene bauen. 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 in einem

Datensatz bemerken DNS-Resolver Aktualisierungen des Datensatzes schneller, da sie häufiger Abfragen erstellen 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:

- Stellen Sie DNS-Datensatz-TTLs für die Dauer ein, die Sie sich leisten können zu warten, bis eine Änderung wirksam wird. Dies gilt insbesondere für Delegierungen (NS-Datensätze) oder andere Datensätze, die sich selten ändern, z. B. MX-Datensätze. Für diese Datensätze werden längere TTLs 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 Zustand überprüft wird), können niedrigere TTLs ausgewählt werden. Das Festlegen einer TTL von 60 oder 120 Sekunden ist eine übliche Wahl für dieses Szenario.
- Wenn Sie Änderungen an kritischen DNS-Einträgen vornehmen möchten, empfehlen wir Ihnen, die 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 Abfragen stellen, um CNAMEs zu beantworten, 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, Routing mit Geoproximität 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 wurden ()`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 Resolver-Verfahren

Folgen Sie diesen bewährten Methoden zur Optimierung von Route 53 Resolver-Verfahren.

Themen

- Vermeiden SieSchleifenkonfigurationenResolver-Endpunkt
- Resolver-Endpunkt-Skalierung
- Hohe Verfügbarkeit für Resolver-Endpunkt
- Gehen Sie zur DNS-Zone

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 VPCs verknüpft werden, die mit anderen Konten gemeinsam genutzt werden. 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. Um die Anzahl der nachverfolgten Verbindungen zu reduzieren, implementieren Sie Sicherheitsgruppenregeln, die Datenverkehr basierend auf dem Verbindungsstatus des Datenverkehrs zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen und Verbindungsverfolgung im Amazon EC2 EC2-Benutzerhandbuch.

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.

Empfehlungen für eingehende und ausgehende Resolver Sicherheitsgruppen

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 Datenverkehr		
Protokolltyp	Port-Nummer	Ziel-IP
TCP	Alle	0.0.0.0/0
UDP	Alle	0.0.0.0/0

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 Route 53-Resolver-Endpunkte erstellen, erfordert Route 53, dass Sie mindestens zwei IP-Adressen erstellen, an die die DNS-Resolver in Ihrem Netzwerk Abfragen 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 unter 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 Team von Route 53 Resolver ein Datenverkehrsmuster erkennt, das mit dem übereinstimmt, das beim Begehen von DNS-Zonen auf Ihrem Endpunkt generiert wird, drosselt das Serviceteam den Datenverkehr auf Ihrem Endpunkt. Als Konsequenz können Sie einen hohen Prozentsatz Ihrer DNS-Abfragen beobachten, der Timeout ist.

Wenn Sie eine reduzierte Kapazität auf Ihren Endgeräten beobachten und glauben, dass der Endpunkt fälschlicherweise gedrosselt wurde, rufen Sie https://console.aws.amazon.com/support/home#/ auf, um einen Supportfall zu erstellen.

Bewährte Methoden für Amazon Route 53 Zustandsprüfungen

Folgen Sie diesen bewährten Methoden zur Optimierung von Amazon Route 53-Zustandsprüfungen.

Themen

Bewährte Methoden für Elastic IP-Adressen für Zustandsprüfungen

Best Practice für Ihre Integritätsprüfungs-Endpunkte ist die Verwendung von Elastic IP-Adressen. Löschen Sie jedoch alle Zustandsprüfungen, die mit einer Elastic IP-Adresse verknüpft sind, die Sie

nicht mehr besitzen. Wenn Sie beispielsweise keine Amazon EC2 Instance mehr verwenden, stellen Sie sicher, dass Sie alle Zustandsprüfungen löschen, die der Elastic IP-Adresse zugeordnet sind. Das liegt daran, dass die Elastic IP-Adresse einem anderen Benutzer zugewiesen werden kann oder dass dadurch Ihre Daten aus dem AWS-Konto Health Check beeinträchtigt werden könnten.

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 zum Anzeigen und Verwalten von Domains, Route 53 und Route-53-Resolver-Kontingenten verwenden.)

> **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 anzufordern, wechseln Sie in die entsprechende 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 Datenverkehrsflussrichtliniendatensätze ab

- GetHostedZoneLimit— Ruft Kontingente für Datensätze in einer gehosteten Zone und auf Amazon-VPCs ab, 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, die Sie mit einer privaten gehosteten Zone verknüpfen können	300 Request a higher quota (Höheres Kontingent anfordern).
Private gehostete Zone, denen Sie eine VPC zuordnen können	Kein Kontingent *
Autorisierungen, die Sie erstellen können, damit Sie VPCs zuordnen können, die mit einem Konto in einer gehosteten Zone erstellt wurden, 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 bei Route 53 Resolver

Dieser Abschnitt enthält alle Quoten der Route 53 Resolver

Kontingente bei Route 53 Resolver

Gehen Sie wie folgt vor, um die Kontingente für Route 53 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 Quota name (Namen des Kontingents) des Route 53-Resolvers, das Sie erhöhen möchten.
4. SelectKontingenterhöhung anfordern, geben Sie den Kontingentwert ein, und wählen Sie dannAnfrageaus.

Kontingente für Route 53 Resolver

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).
Verknüpfungen zwischen Regeln und VPCs pro Region AWS	2000 pro Konto AWS Request a higher quotaf (Höheres Kontingent anfordern).
	10.000*

Entität	Kontingent
UDP-Abfragen pro Sekunde pro IP-Adresse in einem Endpunkt	

* 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. Daher stimmt das QPS für jede ausgehende Netzwerkschnittstelle nicht mit dem an Route 53 Resolver gesendeten QPS überein. Verwenden Sie CloudWatch Metriken, um zu messen, wie viele Anfragen an jede Netzwerkschnittstelle gesendet werden. Weitere Informationen finden Sie unter Metriken für 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 Resolver Abfrageprotokolle

Entität	Kontingent
Abfrageprotokollkonfigurationen pro Region AWS	20
	100

Entität	Kontingent
Abfrageprotokollkonfiguration: VPC-Zuordnungen pro AWS -Region*	
Abfrageprotokollkonfiguration für VPC-Zuordnungen pro Konto pro AWS -Region (freigegeben mit RAM) für das Konto, für das die Konfigura tion freigegeben wurde.	100

* Dies ist ein hartes Limit. Sie können in derselben Datei keine weitere Abfrageprotokollkonfiguration erstellen AWS-Region und ihr weitere 100 VPCs zuordnen.

Route 53 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).
Anzahl der Regeln innerhalb einer Regelgruppe für ein einzelnes Konto pro AWS Region	100 Request a higher quota (Höheres Kontingent anfordern).

Entität	Kontingent
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
c5d.large	Bis zu 7 000
c5d.xlarge	Bis zu 12 000

Instance-Typ	Abfragen pro Sekunde
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
r5.2xlarge	Bis zu 24 000
r5.4xlarge	Bis zu 56 000

Instance-Typ	Abfragen pro Sekunde
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
c5d.4xlarge	Bis zu 30 000
m5.large	Bis zu 5 000

Instance-Typ	Abfragen pro Sekunde
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
r5d.xlarge	Bis zu 10 000*
r5d.2xlarge	Bis zu 18 000

Instance-Typ	Abfragen pro Sekunde
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
Datenfluss-Richtlinien	50 pro AWS Konto

Entität	Kontingent
Weitere Informationen zum Route 53-Datenfluss finden Sie unter Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr.	Request a higher quota (Höheres Kontingent anfordern).
Versionen der Datenverkehrsrichtlinie	1.000 pro Datenverkehrsrichtlinie
Datensätze zu Verkehrsrichtlinien (in der Route 53-API, den AWS SDKs und AWS Tools for Windows PowerShell als „Richtlinieninstanzen“ bezeichnet) AWS Command Line Interface	5 pro Konto AWS 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
Anzahl der Route 53 53-Profile pro AWS-Konto Region	5 Request a higher quotaf (Höheres Kontingent anfordern).

Entität	Kontingent
Anzahl der 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).

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 der Route 53 Resolver API-Anforderungen

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 die 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 der Route 53 Resolver API-Anforderungen

Alle Anforderungen

Fünf Anfragen pro Sekunde pro AWS Konto pro Region. Wenn Sie mehr als fünf Anforderungen pro Sekunde in einer Region senden, gibt 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.

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-Typ im AWS CloudFormation-Benutzerhandbuch – Eine Eigenschaft zur Verwendung von Amazon Route 53 mit AWS CloudFormation, um benutzerdefinierte DNS-Namen für Ihre AWS CloudFormation-Stacks zu erstellen.
- -Diskussionsforen – Ein Community-basiertes für Entwickler, um über technische Fragen zu Route 53 zu diskutieren.
- AWS-Supportcenter – Diese Website stellt Informationen zu Ihren aktuellen Support-Vorgängen und den Ergebnissen aus AWS Trusted Advisor und Zustandsprüfungen, Links zu Diskussionsforen, technische FAQs, das Service Health Dashboard sowie Informationen zu AWS Support-Plänen bereit.
- AWS-Premium-Support-Informationen – Die primäre Webseite für Informationen zu AWS Premium, einem persönlichen und reaktionsschnellen Support-Kanal. Hier erhalten Sie Hilfe bei der Entwicklung und Ausführung von Anwendungen auf AWS Infrastructure Services.
- 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 rollenbasierten und speziellen Kursen sowie Übungen im Selbststudium zur Verbesserung Ihrer AWS-Kompetenzen und Erweiterung Ihrer praktischen Erfahrung.
- AWS-Entwicklerzentrum – Entdecken Sie Tutorials, laden Sie Tools herunter und erfahren Sie mehr über Veranstaltungen für AWS-Entwickler.
- AWS-Entwickler-Tools – Links zu Entwickler-Tools, SDKs, IDE-Toolkits und Befehlszeilen-Tools für die Entwicklung und Verwaltung von AWS-Anwendungen.
- Ressourcenzentrum für die ersten Schritte – Erfahren Sie, wie Sie Ihr AWS-Konto einrichten, der AWS-Community beitreten und Ihre erste Anwendung starten.
- Praktische Tutorials – Schritt-für-Schritt-Anleitungen zum Starten Ihrer ersten Anwendung auf AWS.
- AWS Whitepaper – Links zu einer umfangreichen Liste technischer AWS-Whitepaper zu Themen wie Architektur, Sicherheit und Wirtschaftlichkeit. Diese Whitepaper wurden von AWS-Lösungsarchitekten und anderen technischen Experten verfasst.
- AWS Support-Center – Hub für die Erstellung und Verwaltung Ihrer AWS Support-Fälle. Stellt darüber hinaus Links zu weiteren nützlichen Ressourcen bereit, beispielsweise Foren, häufig gestellten technischen Fragen, Status der Service-Integrität und AWS Trusted Advisor.
- AWS Support – Primäre Website für Informationen zu AWS Support, einem persönlichen und reaktionsschnellen Support-Channel, der Sie bei der Erstellung und Ausführung von Anwendungen in der Cloud unterstützt.
- Kontakt – Zentraler Kontaktpunkt für Fragen zu AWS-Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- Nutzungsbedingungen für die AWS-Website – Detaillierte Informationen zu unseren Copyright- und Markenbestimmungen, Ihrem Konto, den Lizenzen und anderen Themen.

Drittanbieter-Tools und Bibliotheken

Zusätzlich zu den AWS-Ressourcen finden Sie eine Vielzahl von Drittanbieter-Tools und Bibliotheken, die mit Amazon Route 53 verwendet werden können.

- AmazonRoute53AppsScript (über webos-goodies)

  Google-Tabellenverwaltung von Amazon Route 53.
- AWS-Komponente für .NET (über SprightlySoft)

SprightlySoft-.NET-Komponente für Amazon Web Services mit Unterstützung von 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 das Arbeiten 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 von 2024

30. April 2024

Sie können jetzt entscheiden, ob eine DNS-Firewallregel die DNS-Umleitungskette entweder überprüft (Standard) oder ihr vertraut. Weitere Informationen finden Sie unter Route-53-Resolver-DNS-Firewall-Komponenten und -Einstellungen 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 Konten zu teilen. AWS Weitere Informationen finden Sie unter 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 Route 53 Resolver-DNS-Firewallereignissen 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 finden Sie unter Route-53-Resolver-DNS-Firewall-Komponenten und -Einstellungen 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 Routing mit Geoproximität, Spezifische Werte für Datensätze der geografischen Nähe und Spezifische Werte für Geoproximity-Aliasdatensätze.

Veröffentlichungen 2023

20. Dezember 2023

Sie können jetzt DNS über HTTPS mit Route-53-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 Resolver, der alle DNS-Abfragen zwischenspeichert, die vom AWS Outposts stammen. 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 Routing mit Geoproximität 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 AWS-Konto zu übertragen. Weitere Informationen finden Sie unter Registrieren einer neuen Domain und Übertragen von Domänen.

10. März 2023

Sie können jetzt IPv4-, IPv6- oder Dual-Stack-Endpunkte mit Amazon Route 53 Resolver verwenden, um eine Verbindung mit Ihren Ressourcen herzustellen. Weitere Informationen finden 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 Berechtigungen für Ressourcendatensätze.

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 Service AWS App Runner.

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 Supported routing policies for records in a private hosted zone.

25 Januar 2022

Der Prozess zum Ändern des Besitzers für .com.au- und .net.au-TLDs wurde vereinfacht, um auf zwei E-Mails (sowohl von alten als auch von neuen Registranten) zu antworten und beinhaltet kein Ausfüllen von Formularen. Weitere Informationen finden 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 im 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 Verfolgung AWS verwalteter Richtlinien für Amazon Route 53 wurde gestartet. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon Route 53.

31. März 2021

Route 53 Resolver DNS Firewall Mit der DNS-Firewall können Sie Schutz für ausgehende DNS-Anforderungen Ihrer VPCs bieten. Weitere Informationen finden Sie unter Route 53 Resolver DNS Firewall.

Versionspunkte 2020

17. Dezember 2020

Unterstützung für DNSSEC-Signierung für Route 53 Resolver hinzugefügt. Weitere Informationen finden Sie unter Konfigurieren der DNSSEC-Signatur in Amazon Route 53.

Unterstützung für DNSSEC-Validierung für Route 53 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-Alias-Datensätze 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? Amazon Route 53 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 Routing mit Geoproximität.

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 Domäne registrieren, erfordern die Registrierungen für einige Top Level Domains (TLDs), dass Sie prüfen, ob Sie eine gültige E-Mail-Adresse für den Registriererkontakt 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 Zustandsprüfungen erstellen, die IPv6-Adressen verwenden, um den Zustand der Endpunkte 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. Ein häufiges Beispiel ist 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. Bei Geolocation- und Latenz-Datensätzen können Sie außerdem Abfragen von einem bestimmten DNS-Resolver und/oder einer Client-IP-Adresse auch simulieren, um herauszufinden, welche Antwort Route 53 an einen Client mit diesem Resolver und/oder dieser IP-Adresse zurückgibt. 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 Domänenregistrierungsvorgänge, für die es eine Gebühr gibt, einschließlich der Registrierung von Domänen, Übertragen von Domänen an Route 53, Erneuerung der Domänenregistrierung und (für einige TLDs) Ändern des Besitzers der Domäne. 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.
- Neue TLDs - Sie können jetzt Domänen mit den folgenden TLDs registrieren: .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.

- Neue APIs für die Domänenregistrierung - Für Vorgänge, die eine Bestätigung erfordern, dass die E-Mail-Adresse des Registrierenden gültig ist, wie zum Beispiel bei einer Registrierung einer neuen Domäne, können Sie jetzt programmgesteuert bestimmen, ob der Registrierende 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 Health checker regions 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. Damit kann der Endpunkt auf die HTTPS-Anforderung mit dem entsprechenden SSL/TLS-Zertifikat reagieren. Weitere Informationen finden Sie in der Beschreibung für das Feld Enable SNI im Thema "Angegebene Werte beim Erstellen oder Aktualisieren von Zustandsprüfungen". 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 Domänen für mehr als 100 zusätzliche Top-Level-Domänen (TLDs) registrieren, wie z. B. .accountants, .band, .city. Eine vollständige Liste der unterstützten TLD finden Sie unter 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, die AWS SDKs AWS CLI, und AWS Tools for Windows PowerShell verwenden. Weitere Informationen zur Verwendung des visuellen Editors finden Sie unter Verwendung des Datenverkehrsflusses zum Weiterleiten von DNS-Datenverkehr. 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:

- Domänenregistrierung für .com- und .net-Domänen von Amazon Registrar, Inc. – Amazon ist jetzt eine von ICANN autorisierte Vergabestelle für .com- und .net-Top-Level-Domänen (TLDs) über Amazon Registrar, Inc. Wenn Sie mithilfe von Route 53 eine .com- oder .net-Domäne registrieren, ist Amazon Registrar die Vergabestelle des Eintrags und wird als "Sponsoring Registrar" in den Whois-Abfragen aufgelistet. 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:

- Private DNS für VPCs, die mithilfe des Amazon Virtual Private Cloud-Service erstellt wurden - Sie können jetzt mithilfe von Route 53 Ihre internen Domänennamen für VPCs verwalten, ohne dass die DNS-Namen im öffentlichen Internet bekannt werden. 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 edns-client-subnet Erweiterung von EDNS0 hinzugefügt haben. 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 eine Endpunkt-IP-Adresse entweder nicht feststeht oder von mehreren IP-Adressen bedient wird, wie z. B. Amazon EC2- oder Amazon RDS-Instances. 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

Ab dieser Version fügt Route 53 Unterstützung für die Bewertung des Zustands von ELB Load Balancers und den zugehörigen Amazon EC2-Instances hinzu. Weitere Informationen finden Sie unter Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

28. März 2013

Die Dokumentation zu Zustandsprüfungen und Failover wurde für bessere Benutzerfreundlichkeit umgeschrieben. Weitere Informationen finden Sie unter Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

11. Februar 2013

Ab dieser Version fügt Route 53 Unterstützung für Failover und Zustandsprüfungen hinzu. Weitere Informationen finden Sie unter Erstellen von Amazon Route 53-Zustandsprüfungen und Konfigurieren des DNS Failovers.

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 Management Console 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 Management Console 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.

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.