aws

Guida per gli sviluppatori

Amazon Route 53

Versione API 2013-04-01

Amazon Route 53: Guida per gli sviluppatori

Table of Contents

Che cos'è Amazon Route 53?

Amazon Route 53 è un servizio Web DNS (Domain Name System) altamente scalabile e disponibile. Puoi utilizzare Route 53 per eseguire tre funzioni principali in qualsiasi combinazione: registrazione dominio, routing DNS e controllo dell'integrità.

Se scegli di utilizzare Route 53 per tutte le tre funzioni, assicurati di seguire l'ordine riportato di seguito:

1. Registrazione di nomi di dominio

   Il tuo sito Web ha bisogno di un nome, ad esempio esempio.com. Route 53 ti consente di registrare un nome per il tuo sito o applicazione Web, noto come nome di dominio.

   - Per una panoramica, consulta Come funziona la registrazione dei domini.
   - Per una procedura, vedi Registrazione di un nuovo dominio.
   - Per un tutorial che guidi l'utente attraverso la registrazione di un dominio e la creazione di un sito Web semplice in un bucket Amazon S3, consulta Nozioni di base su Amazon Route 53.

2. Instradare il traffico Internet verso le risorse per il tuo dominio

   Quando un utente apre un browser Web e immette il tuo nome di dominio (esempio.com) o un nome di sottodominio (acme.esempio.com) nella barra degli indirizzi, Route 53 consente di collegare il browser con il tuo sito o applicazione Web.

   - Per una panoramica, consulta In che modo il traffico Internet viene instradato al tuo sito o applicazione Web.
   - Per le procedure, consulta Configurazione di Amazon Route 53 come servizio DNS.
   - Per una procedura su come indirizzare le e-mail ad Amazon WorkMail, consultaInstradamento del traffico verso Amazon WorkMail.

3. Controlla lo stato delle tue risorse

   Route 53 invia richieste automatizzate tramite Internet a una risorsa, ad esempio un server Web, per verificare che sia raggiungibile, disponibile e funzionante. Puoi anche scegliere di ricevere notifiche quando una risorsa non è più disponibile e scegliere di instradare il traffico Internet lontano da risorse non integre.

   - Per una panoramica, consulta Come Amazon Route 53 controlla l'integrità delle risorse.
   - Per le procedure, consulta Creazione di controlli sanitari su Amazon Route 53 .

Altre funzionalità della Route 53

Oltre a essere un servizio web DNS (Domain Name System), Route 53 offre le seguenti funzionalità:

Route 53 Resolver

Ottieni DNS ricorsivo per il tuo Amazon VPCs in Regioni AWS, in AWS Outposts rack o VPCs in qualsiasi altra rete locale. Crea regole di inoltro condizionale ed endpoint Route 53 per risolvere i nomi personalizzati gestiti nelle zone ospitate private di Route 53 o nei tuoi server DNS locali.

Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.

Amazon Route 53 Resolver su Outposts

Connetti Route 53 Resolver sui rack Outpost con i server DNS nei data center locali tramite gli endpoint Route 53 Resolver. Ciò consente la risoluzione delle query DNS tra i rack Outposts e le altre risorse locali.

Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 on Outposts?.

DNS Firewall per Route 53 Resolver

Proteggi le tue query DNS ricorsive all'interno del Route 53 Resolver. Crea elenchi di domini e crea regole firewall che filtrano il traffico DNS in uscita in base a queste regole.

Per ulteriori informazioni, consulta Utilizzo di DNS Firewall per filtrare il traffico DNS in uscita.

Flusso di traffico

Easy-to-use e una gestione del traffico globale a costi contenuti: indirizza gli utenti finali verso l'endpoint migliore per la tua applicazione in base a geoprossimità, latenza, integrità e altre considerazioni.

Per ulteriori informazioni, consulta Utilizzo di Traffic Flow per instradare il traffico DNS.

Profili di Amazon Route 53

Con Route 53 Profiles, puoi applicare e gestire configurazioni Route 53 relative al DNS su molte configurazioni VPCs e in diversi modi. Account AWS

Per ulteriori informazioni, consulta Cosa sono i profili Amazon Route 53?.

Argomenti

- In che modo il traffico Internet viene instradato al tuo sito o applicazione Web
- Come Amazon Route 53 controlla l'integrità delle risorse
- Nozioni di Amazon Route 53
- Nozioni di base su Amazon Route 53
- Accesso a Amazon Route 53
- AWS Identity and Access Management
- Prezzi e fatturazione di Amazon Route 53
- Utilizzo di Route 53 con un SDK AWS

Come funziona la registrazione dei domini

Se desideri creare un sito Web o un'applicazione Web, puoi iniziare registrando il nome del tuo sito Web, noto come domain name. Il tuo nome di dominio è il nome, ad esempio esempio.com, che gli utenti immettono in un browser per visualizzare il tuo sito Web.

Ecco una panoramica di come effettuare la registrazione di un nome di dominio con Amazon Route 53:

1. Puoi scegliere un nome di dominio e confermare che è disponibile, il che significa che nessun altro ha registrato il nome di dominio che desideri.

   Se il nome di dominio desiderato è già in uso, puoi provare altri nomi o provare a modificare solo il dominio di livello superiore, ad esempio .com, con un altro dominio di livello superiore, ad esempio.ninja o.hockey. Per un elenco dei domini di primo livello supportati da Route 53, consulta Domini che è possibile registrare con Amazon Route 53.
2. Registra il nome di dominio con Route 53. Quando record un dominio, devi fornire nomi e informazioni di contatto del proprietario del dominio e altri contatti.

   Quando record un dominio con Route 53, il servizio diventa automaticamente il servizio DNS per il dominio eseguendo le operazioni seguenti:

   - Crea un hosted zone con lo stesso nome del tuo dominio.
   - Assegna un set di quattro nomi di server alla zona ospitata. Quando un utente utilizza un browser per accedere al tuo sito Web, ad esempio www.example.com, questi server di nomi indicano al browser dove trovare le tue risorse, come un server Web o un bucket Amazon S3. (Amazon S3 è l'archiviazione di oggetti che consente di archiviare e recuperare qualsiasi

quantità di dati in qualsiasi luogo tramite il Web. Un bucket è un container per gli oggetti che archivi in S3.)

- Ottiene il server di nomi dalla zona ospitata e li aggiunge al dominio.

Per ulteriori informazioni, consulta In che modo il traffico Internet viene instradato al tuo sito o applicazione Web.

3. Al termine del processo di registrazione, inviamo le tue informazioni al registrar per il dominio. Il domain registrar è Amazon Registrar, Inc. o il registrar associato, Gandi. Per stabilire chi è il registrar per il tuo dominio, consulta Ricerca del registrar.
4. Il registrar invia le informazioni al record per il dominio. Un registro è una società che vende registrazioni di dominio per uno o più domini di primo livello, come ad esempio .com.
5. Il record memorizza le informazioni sul tuo dominio nel proprio database e memorizza anche alcune delle informazioni nel database WHOIS pubblico.

Per ulteriori informazioni su come eseguire la registrazione di un nome di dominio, consulta Registrazione di un nuovo dominio.

Se hai già registrato un nome di dominio con un altro registrar, puoi decidere di trasferire la registrazione di dominio a Route 53. Questo non è necessario per l'utilizzo delle altre caratteristiche di Route 53. Per ulteriori informazioni, consulta Trasferimento della registrazione per un dominio ad Amazon Route 53.

In che modo il traffico Internet viene instradato al tuo sito o applicazione Web

Tutti i computer su Internet, dallo smartphone o dal laptop, si connettono ai server che forniscono contenuti per grandi siti di vendita al dettaglio e comunicano tra loro tramite numeri. Questi numeri, noti come indirizzi IP, sono in uno dei seguenti formati:

- Formato Internet Protocol versione 4 (IPv4), ad esempio 192.0.2.44
- Formato Internet Protocol versione 6 (IPv6), ad esempio 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345

Quando apri un browser e accedi a un sito Web, non devi ricordare e inserire una stringa di caratteri così lunga. Puoi semplicemente inserire un nome di dominio come esempio.com e arrivare

comunque al posto giusto. Un servizio DNS come Amazon Route 53 contribuisce a creare tale connessione tra i nomi di dominio e gli indirizzi IP.

Argomenti

Panoramica di come configurare Amazon Route 53 per instradare il traffico Internet per il tuo dominio

Ecco una panoramica di come utilizzare la console Amazon Route 53 per registrare un nome di dominio e configurare Route 53 per instradare il traffico Internet verso il tuo sito o applicazione Web.

1. Puoi registrare il nome di dominio che desideri utilizzare per accedere ai tuoi contenuti. Per una panoramica, consulta Come funziona la registrazione dei domini.
2. Dopo aver registrato il tuo nome di dominio, Route 53 crea automaticamente una zona ospitata pubblica con lo stesso nome del dominio. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate pubbliche.
3. Per instradare il traffico verso le tue risorse devi creare record, noti anche come set di record di risorse, nella tua zona ospitata. Ogni record include informazioni su come desideri instradare il traffico per il tuo dominio, ad esempio:

   Nome

   Il nome del record corrisponde al nome di dominio (esempio.com) o di sottodominio (www.esempio.com, retail.esempio.com) a cui desideri che Route 53 instradi il traffico.

   Il nome di ogni record in una zona ospitata deve terminare con il nome della zona ospitata. Ad esempio, se il nome della zona ospitata è esempio.com, tutti i nomi di record devono terminare in esempio.com. La console Route 53 fa tutto questo automaticamente.

   Tipo

   Il tipo di record in genere determina il tipo di risorsa a cui desideri che il traffico venga instradato. Ad esempio, per instradare il traffico a un server e-mail, devi specificare MX per Type (Tipo). Per indirizzare il traffico verso un server Web che dispone di un indirizzo IP, specificate A per Tipo. IPv4

Valore

Il valore è strettamente correlato al tipo. Se specifichi MX per Type (Tipo), devi specificare i nomi di uno o più server di e-mail per Value (Valore). Se si specifica A per Tipo, si specifica un indirizzo IP in IPv4 formato, ad esempio 192.0.2.136.

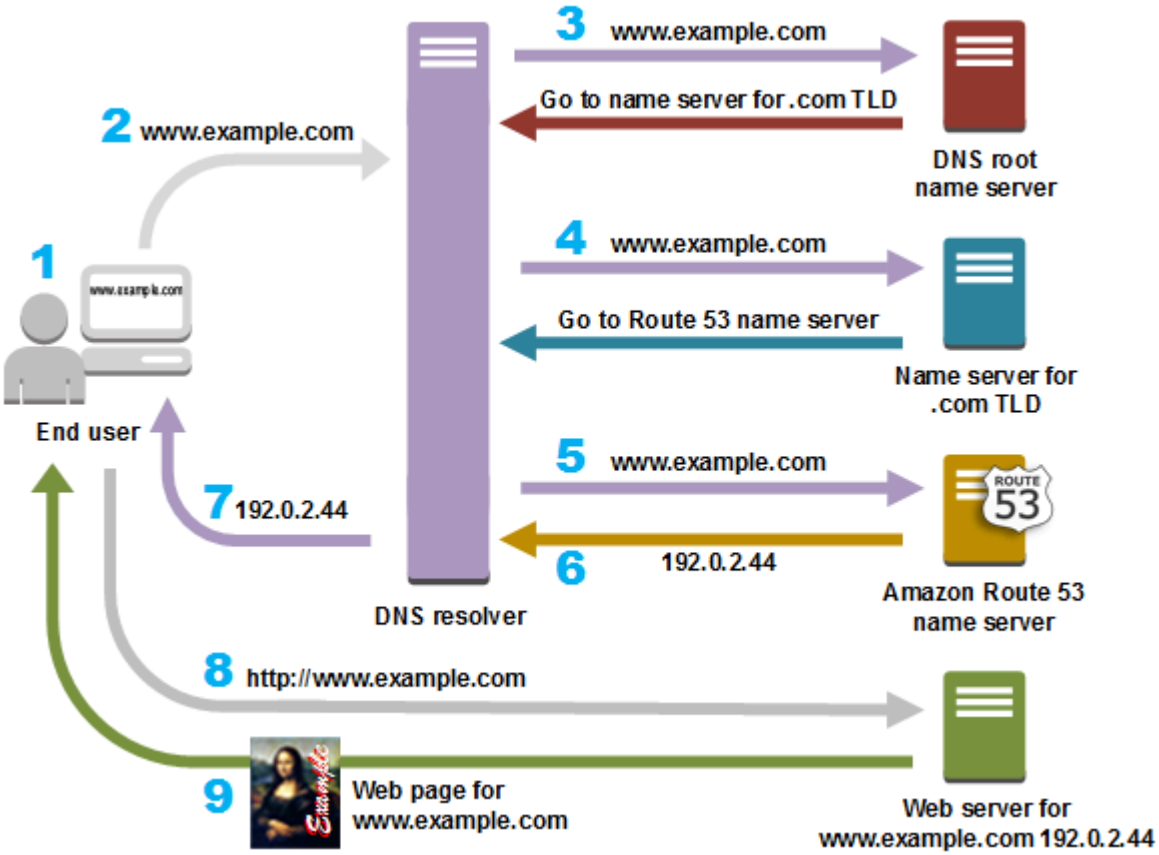
Per ulteriori informazioni sul record, consulta Utilizzo dei record.

Puoi anche creare record Route 53 speciali, chiamati record alias, che indirizzano il traffico verso i bucket Amazon S3, le distribuzioni CloudFront Amazon e altre risorse. AWS Per ulteriori informazioni, consulta Scelta tra record alias e non alias e Instradamento del traffico Internet verso le tue risorse AWS.

Per ulteriori informazioni su come instradare il traffico Internet verso le tue risorse, consulta Configurazione di Amazon Route 53 come servizio DNS.

Come Amazon Route 53 instrada il traffico per il tuo dominio

Dopo aver configurato Amazon Route 53 per instradare il traffico Internet verso le tue risorse, ad esempio server Web o bucket Amazon S3, ecco cosa succede in pochi millisecondi quando qualcuno richiede contenuti per www.esempio.com:



1. Un utente apre un browser Web, inserisce www.esempio.com nella barra degli indirizzi e preme Invio.
2. La richiesta per www.esempio.com è indirizzata a un resolver DNS, tipicamente gestito dal provider di servizi Internet (ISP) dell'utente, come un provider internet via cavo, un provider di banda larga DSL o una rete aziendale.
3. Il resolver DNS per l'ISP inoltra la richiesta per www.esempio.com a un server dei nomi root DNS.
4. Il resolver DNS inoltra la richiesta per www.esempio.com nuovamente, questa volta a uno dei server dei nomi TLD per i domini .com. Il server dei nomi per i domini .com risponde alla richiesta con i nomi dei quattro server dei nomi di Route 53 associati al dominio esempio.com.

   Il resolver DNS memorizza nella cache (archivia) i quattro server dei nomi di Route 53. La volta successiva che una persona accede a esempio.com, il resolver salta i passaggi 3 e 4 perché dispone già dei server dei nomi per esempio.com. Il server di nomi sono in genere memorizzati nella cache per due giorni.
5. Il resolver DNS sceglie un server dei nomi di Route 53 e inoltra la richiesta per www.esempio.com a quel server dei nomi.

6. Il server dei nomi di Route 53 cerca nella zona ospitata esempio.com il record www.esempio.com, ottiene il valore associato, come l'indirizzo IP per un server Web 192.0.2.44, e restituisce l'indirizzo IP al resolver DNS.
7. Il resolver DNS ottiene così l' indirizzo IP di cui l'utente ha bisogno. Il resolver restituisce tale valore al browser Web.

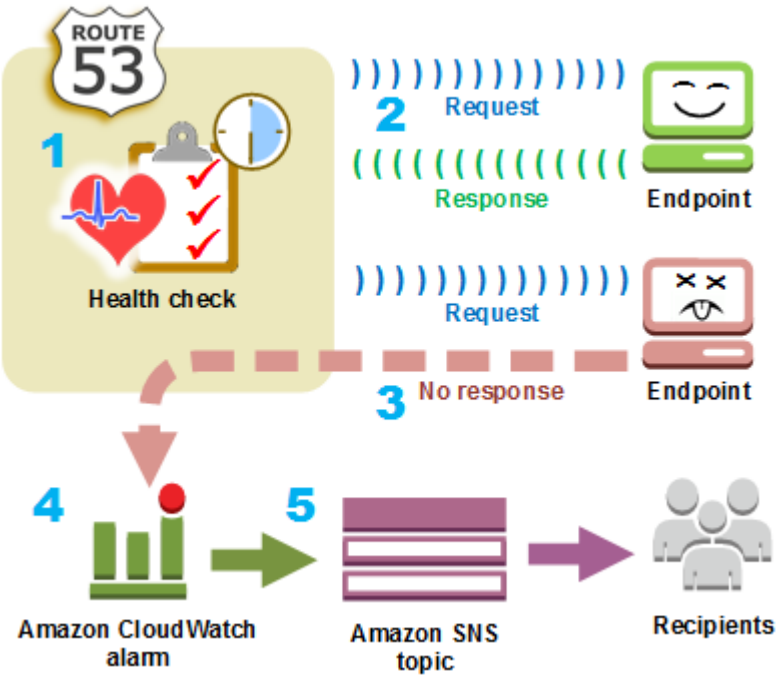
> **Note**
>
> Il resolver DNS memorizza nella cache anche l'indirizzo IP per esempio.com per un periodo di tempo specificato in modo che possa rispondere più rapidamente la prossima volta che qualcuno accede a esempio.com. Per ulteriori informazioni, consulta time to live (TTL).

8. Il browser Web invia una richiesta per www.esempio.com all'indirizzo IP ottenuto dal resolver DNS. È qui che i tuoi contenuti sono, ad esempio, un server Web in esecuzione su un' EC2 istanza Amazon o un bucket Amazon S3 configurato come endpoint del sito Web.
9. Il server web o altra risorsa presso 192.0.2.44 restituisce la pagina web per www.esempio.com al browser web, e il browser web visualizza la pagina.

Come Amazon Route 53 controlla l'integrità delle risorse

I controlli dell'integrità di Amazon Route 53 monitorano lo stato delle risorse come i server Web e i server di posta elettronica. Facoltativamente, puoi configurare gli CloudWatch allarmi Amazon per i tuoi controlli sanitari, in modo da ricevere una notifica quando una risorsa diventa non disponibile.

Ecco una panoramica sul funzionamento dei controlli dell'integrità se desideri ricevere una notifica quando una risorsa non è più disponibile:



1. Puoi creare un controllo dell'integrità e specificare i valori che definiscono il modo in cui desideri che funzioni, come ad esempio:
   - L'indirizzo IP o il nome di dominio dell'endpoint, ad esempio un server Web, che desideri sia monitorato da Route 53. (Puoi anche monitorare lo stato di altri controlli sanitari o lo stato di un CloudWatch allarme.)
   - Il protocollo che si desidera che Amazon Route 53 da usare per eseguire il check: HTTP, HTTPS o TCP.
   - Con quale frequenza desideri che Route 53 invii una richiesta all'endpoint. Questo è l'intervallo di richiesta.
   - Quante volte consecutive l'endpoint non deve essere in grado di rispondere alle richieste prima che Route 53 lo consideri non integro. Questa è la soglia di errore.
   - Facoltativamente, il modo in cui desideri ricevere una notifica quando Route 53 rileva che l'endpoint non è integro. Quando configuri la notifica, Route 53 imposta automaticamente un CloudWatch allarme. CloudWatch utilizza Amazon SNS per notificare agli utenti che un endpoint non è integro.
2. Route 53 inizia a inviare le richieste all'endpoint in base all'intervallo di tempo specificato nel controllo dell'integrità.

   Se l'endpoint risponde alle richieste, Route 53 considera gli endpoint integri e non viene eseguita alcuna operazione.

3. Se l'endpoint non risponde a una richiesta, Route 53 inizia a contare il numero di richieste consecutive a cui l'endpoint non risponde:
   - Se il conteggio raggiunge il valore specificato per la soglia di errore, Route 53 considera l'endpoint non integro.
   - Se l'endpoint ricomincia a rispondere prima che il conteggio raggiunga la soglia di errore, Route 53 reimposta il conteggio a 0 e CloudWatch non ti contatta.
4. Se Route 53 ritiene che l'endpoint non sia integro e se hai configurato una notifica per il controllo dello stato, Route 53 invia una notifica. CloudWatch

   Se non hai configurato le notifiche, puoi comunque consultare lo stato dei controlli dell'integrità di Route 53 nella console Route 53. Per ulteriori informazioni, consulta Monitoraggio dello stato del controllo dell'integrità e ricezione di notifiche.
5. Se hai configurato la notifica per il controllo dello stato, CloudWatch attiva un allarme e utilizza Amazon SNS per inviare notifiche ai destinatari specificati.

Oltre a controllare lo stato di un endpoint specificato, puoi configurare un controllo dell'integrità per controllare lo stato di uno o più altri controlli dell'integrità in modo che sia possibile ricevere una notifica quando un determinato numero di risorse, ad esempio due server Web su cinque, non sono disponibili. Puoi anche configurare un controllo sanitario per verificare lo stato di un CloudWatch allarme in modo da ricevere una notifica in base a un'ampia gamma di criteri, non solo se una risorsa sta rispondendo alle richieste.

Se disponi di più risorse che eseguono la stessa funzione, ad esempio server Web o server di database e desideri che Route 53 instradi il traffico solo alle risorse che sono integre, puoi configurare il failover DNS associando un controllo dell'integrità a ogni record per la risorsa. Se un controllo dell'integrità determina che la risorsa sottostante è integra, Route 53 indirizza il traffico dal record associato.

Per ulteriori informazioni su come usare Route 53 per monitorare l'integrità delle tue risorse, consulta Creazione di controlli sanitari su Amazon Route 53 .

Nozioni di Amazon Route 53

Ecco una panoramica delle nozioni che vengono discusse nella Guida per gli sviluppatori di Amazon Route 53.

Argomenti

- Concetti sulla registrazione dei domini
- Concetti su DNS (Domain Name System)
- Nozioni sul piano di controllo e sul piano dati
- Concetti sul controllo dell'integrità

Concetti sulla registrazione dei domini

Ecco una panoramica delle nozioni relative alla registrazione di domini.

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

nome di dominio

Il nome, ad esempio esempio.com, che un utente digita nella barra degli indirizzi di un browser Web per accedere a un sito Web o un'applicazione Web. Per rendere il tuo sito o applicazione Web disponibile su Internet, puoi iniziare registrando un nome di dominio. Per ulteriori informazioni, consulta Come funziona la registrazione dei domini.

registrar di dominio

Una società accreditata dall'ICANN (Internet Corporation for Assigned Names and Numbers) per elaborare le registrazioni di domini per domini di primo livello specifici (). TLDs Per stabilire chi è il registrar per il tuo dominio, consulta Ricerca del registrar.

record di dominio

Un'azienda possiede il diritto di vedere domini che hanno un dominio di primo livello specifico. Ad esempio, VeriSignè il registro che detiene il diritto di vendere domini con un TLD.com. Un database del record di dominio definisce le regole per la registrazione di un dominio, ad esempio i requisiti di residenza per un TLD geografico. Un record di dominio, inoltre, mantiene l'autorevole database per tutti i nomi di domini con lo stesso TLD. Il database del registro contiene informazioni quali dati di contatto e i server dei nomi per ogni dominio.

rivenditore didominio

Un'azienda che vende nomi di dominio per registrar come Amazon Registrar. Amazon Route 53 è un rivenditore di domini per Amazon Registrar e per il nostro registrar associato, Gandi.

dominio di primo livello (TLD)

L'ultima parte di un nome di dominio, ad esempio .com, .org o .ninja. Sono disponibili due tipi di domini di primo livello:

Domini di primo livello generici

Questi TLDs in genere danno agli utenti un'idea di ciò che troveranno sul sito Web. Ad esempio, i nomi di dominio che dispongono di un TLD .bike spesso sono associati a siti Web di aziende o organizzazioni di motociclette o biciclette. Con pochi eccezioni, è possibile usare qualsiasi TLD generico desiderato, quindi un club ciclistico potrebbe utilizzare il TLD .hockey per il proprio nome di dominio.

Domini di primo livello geografici

Questi TLDs sono associati ad aree geografiche come paesi o città. Alcuni registri geografici TLDs prevedono requisiti di residenza, mentre altri, ad esempiothe section called ".io (Territorio britannico dell'Oceano Indiano)", consentono o addirittura incoraggiano l'uso come dominio di primo livello generico.

Per un elenco di quelli TLDs che puoi usare quando registri un nome di dominio con Route 53, vedi. Domini che è possibile registrare con Amazon Route 53

Concetti su DNS (Domain Name System)

Ecco una panoramica delle nozioni relative al 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)

record alias

Un tipo di record che puoi creare con Amazon Route 53 per indirizzare il traffico verso AWS risorse come le CloudFront distribuzioni Amazon e i bucket Amazon S3. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

server di nomi ufficiale

Un server di nomi che ha informazioni ufficiali su una parte del DNS (Domain Name System) e che risponde alle richieste di un resolver DNS restituendo le informazioni applicabili. Ad esempio, un server i nomi ufficiale per il dominio di primo livello (TLD) .com conosce i nomi dei server di nomi per ogni nome di dominio .com registrato. Quando un server di nomi ufficiale .com riceve una richiesta da un resolver DNS per esempio.com, risponde con i nomi del server di nomi per il servizio DNS per il dominio esempio.com.

I server dei nomi di Route 53 sono server dei nomi ufficiali per ogni dominio che utilizza Route 53 come servizio DNS. I server di nomi sanno come desideri instradare il traffico per il tuo dominio e i sottodomini in base ai record creati nella hosted zone per il dominio. (I server dei nomi di Route 53 archiviano le zone ospitate per i domini che utilizzano Route 53 come servizio DNS.)

Ad esempio, se un server dei nomi di Route 53 riceve una richiesta per www.esempio.com, trova il record e restituisce l'indirizzo IP, ad esempio 192.0.2.33, specificato nel record.

blocco CIDR

Un blocco CIDR è un intervallo IP utilizzato con il routing basato su IP. In Route 53 puoi specificare un blocco CIDR da /0 a /24 per e/0 a /48 per. IPv4 IPv6 Ad esempio, un blocco IPv4 CIDR /24 include 256 indirizzi IP contigui. Puoi raggruppare i set di blocchi CIDR (o gli intervalli IP) in posizioni CIDR, che a loro volta vengono raggruppate in raccolte CIDR riutilizzabili.

query DNS

Di solito una richiesta che è stata inviata da un dispositivo come un computer o uno smartphone, al DNS (Domain Name System) per una risorsa che è associata a un nome di dominio. L'esempio più comune di una query DNS è quando un utente apre un browser e digita il nome di dominio nella barra degli indirizzi. La risposta a una query DNS in genere è l'indirizzo IP associato a una risorsa, ad esempio un server Web. Il dispositivo che ha avviato la richiesta utilizza l'indirizzo IP per comunicare con la risorsa. Ad esempio, un browser può utilizzare l'indirizzo IP per ottenere una pagina Web da un server Web.

resolver DNS

Un server DNS, spesso gestito da un fornitore di servizi Internet (ISP), che funge da intermediario tra le richieste degli utenti e i server di nomi DNS. Quando si apre un browser e si digita un nome di dominio nella barra degli indirizzi, la query va prima a un resolver DNS. Il resolver comunica con i server di nomi DNS per ottenere l'indirizzo IP per la risorsa corrispondente, ad esempio un server Web. Un resolver DNS è noto anche come un server di nomi ricorsivo perché invia le richieste a una sequenza di server di nomi DNS ufficiali fino a che non ottiene la risposta (normalmente un indirizzo IP) che restituisce al dispositivo di un utente, ad esempio, un browser Web su un computer portatile.

Domain Name System (DNS)

Una rete globale di server che aiutano computer, smartphone, tablet e altri dispositivi dotati di IP a comunicare tra loro. Il DNS (Domain Name System) traduce i nomi di facile comprensione, ad esempio esempio.com, in numeri, noti come indirizzi IP, che consentono ai computer di individuarsi su Internet.

Consulta anche IP address.

hosted zone

Un container per i record, che includono informazioni su come si desidera instradare il traffico per un dominio (ad esempio esempio.com) e tutti i suoi sottodomini (ad esempio www.esempio.com, retail.esempio.com e seattle.accounting.esempio.com). Una zona ospitata ha lo stesso nome del dominio corrispondente.

Ad esempio, la zona ospitata per esempio.com potrebbe includere un record che dispone di informazioni sul routing del traffico per www.esempio.com a un server Web con l'indirizzo IP 192.0.2.243 e un record che dispone di informazioni sul routing di e-mail per esempio.com a due server di posta elettronica, mail1.esempio.com e mail2.esempio.com. Ogni server di posta elettronica, inoltre, richiede il proprio record.

Consulta anche record (DNS record).

Indirizzo IP

Un numero assegnato a un dispositivo su Internet, ad esempio un portatile, uno smartphone o un server Web, che consente al dispositivo di comunicare con altri dispositivi su Internet. Gli indirizzi IP sono in uno dei seguenti formati:

- Formato Internet Protocol versione 4 (IPv4), ad esempio 192.0.2.44
- Formato Internet Protocol versione 6 (IPv6), ad esempio 2001:0 db 8:85 a 3:0000:0000:abcd:0001:2345

Route IPv4 53 supporta entrambi gli indirizzi D per i seguenti scopi: IPv6

- È possibile creare record con un tipo A, per IPv4 gli indirizzi, o un tipo di AAAA, per IPv6 gli indirizzi.
- È possibile creare controlli sanitari che inviano richieste a IPv4 o verso IPv6 indirizzi.
- Se un resolver DNS si trova su una IPv6 rete, può utilizzare uno dei due IPv4 o inviare richieste IPv6 a Route 53.

server di nomi

Server nel Domain Name Systems (DNS) che consentono di tradurre i nomi di dominio in indirizzi IP che i computer impiegano per comunicare tra loro. I server di nomi sono server di nomi ricorsivi (noti anche come DNS resolver) o authoritative name server.

Per una panoramica di come DNS instrada il traffico verso le tue risorse, incluso il ruolo di Route 53 nel processo, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

DNS privato

Una versione locale del Domain Name System (DNS) che consente di indirizzare il traffico per un dominio e i relativi sottodomini verso EC2 istanze Amazon all'interno di uno o più cloud privati virtuali Amazon (). VPCs Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.

record (record DNS)

Un oggetto in una zona ospitata utilizzato per definire il modo in cui desideri instradare il traffico per il dominio o un sottodominio. Ad esempio, puoi creare record per esempio.com e www.esempio.com che instradano il traffico a un server Web con un indirizzo IP di 192.0.2.234.

Per ulteriori informazioni sui record, tra cui informazioni sulle funzionalità offerte da record specifici di Route 53, consulta Configurazione di Amazon Route 53 come servizio DNS.

server di nomi ricorsivi

Per informazioni, consulta DNS resolver.

set di deleghe riutilizzabile

Un set di quattro server di nomi ufficiali che è possibile utilizzare con più di una zona ospitata. Per impostazione predefinita, Route 53 assegna una selezione casuale di server di nomi a ciascuna nuova zona ospitata. Per semplificare la migrazione del servizio DNS a Route 53 per un numero elevato di domini, è possibile creare un set di delega riutilizzabile e quindi associarlo a nuove zone ospitate. (Non puoi modificare i server di nomi che sono associati a una zona ospitata esistente).

Puoi creare un set di delega riutilizzabile e associarlo una zona ospitata in modo programmatico; l'utilizzo della console Route 53 non è supportato. Per ulteriori informazioni, consulta CreateHostedZonee CreateReusableDelegationSetconsulta Amazon Route 53 API Reference. La stessa funzionalità è disponibile anche in AWS SDKs, AWS Command Line Interface, e AWS Tools for Windows PowerShell.

policy di routing

Una impostazione per i record che determina come Route 53 risponde alle query DNS. Route 53 supporta le seguenti policy di routing:

- Policy di routing semplice: utilizza questa opzione per instradare il traffico Internet a una singola risorsa che esegue una determinata funzione per il tuo dominio, ad esempio un server Web che fornisce i contenuti per il sito Web esempio.com.
- Policy di routing di failover: utilizza questa opzione se desideri configurare un failover attivo-passivo.
- Policy di routing di geolocalizzazione: utilizza questa opzione per instradare il traffico Internet alle proprie risorse in base alla posizione degli utenti.
- Policy di routing di geolocalizzazione: utilizza questa opzione se desideri instradare il traffico in base alla posizione delle tue risorse e, facoltativamente, spostare il traffico dalle risorse in una posizione alle risorse in un'altra.
- Policy di routing di latenza: utilizza questa opzione nel caso in cui si hanno risorse in più posizioni e si desidera instradare il traffico alla risorsa che offre la migliore latenza.
- Policy di routing basato su IP: utilizza questa opzione quando desideri instradare il traffico in base alle posizioni degli utenti e disporre degli indirizzi IP da cui proviene il traffico.
- Policy di routing con risposta multivalore: utilizza questa opzione se desideri che Route 53 risponda alle query DNS con un massimo di otto record integri selezionati casualmente.

- Policy di routing ponderata: utilizza questa opzione se desideri instradare il traffico a più risorse nelle proporzioni specificate.

Per ulteriori informazioni, consulta Scegliere una policy di routing.

sottodominio

Un nome di dominio che dispone di una o più etichette anteposte al nome di dominio registrato. Ad esempio, se record il nome di dominio esempio.com, www.esempio.com è un sottodominio. Se crei la zona ospitata accounting.esempio.com per il dominio esempio.com, seattle.accounting.esempio.com è un sottodominio.

Per instradare il traffico per un sottodominio, devi creare un record con il nome desiderato, ad esempio www.esempio.com, e specificare i valori applicabili, ad esempio l'indirizzo IP di un server Web.

time to live (TTL)

La quantità di tempo, in secondi, per cui si desidera che un resolver DNS memorizzi nella cache (archivi) i valori per un record prima di inviare un'altra richiesta a Route 53 per ottenere i valori correnti per quel record. Se il resolver DNS riceve un'altra richiesta per lo stesso dominio prima della scadenza del TTL, il resolver restituisce il valore memorizzato nella cache.

Un TTL più lungo consente di ridurre i costi di Route 53, che sono basati in parte sul numero di query DNS a cui Route 53 risponde. Un TTL più breve riduce la quantità di tempo che il resolver DNS impiega per instradare il traffico alle risorse più vecchie dopo aver modificato i valori in un record, ad esempio cambiando l' indirizzo IP per il server web per www.esempio.com.

Nozioni sul piano di controllo e sul piano dati

Ecco una panoramica sulle nozioni riguardanti le modalità in cui Amazon Route 53 separa le proprie funzionalità in un piano di controllo e un piano dati. Come molti Servizi AWS, il servizio Route 53 comprende un piano di controllo che permette operazioni di gestione come creare, aggiornare e rimuovere risorse, con un piano dati che provvede alle funzionalità principali del servizio. Mentre entrambe le funzionalità sono state progettate per garantire una maggiore affidabilità, i piani di controllo sono stati ottimizzati per la coerenza dei dati e i piani dati per la disponibilità degli stessi. Grazie al suo design resiliente, il piano dati può mantenere la disponibilità persino durante rari eventi di disturbo, quando è possibile che il piano di controllo non sia più disponibile. Ecco perché raccomandiamo l'uso di funzioni del piano dati quando la disponibilità è importante.

Per i controlli DNS e sanitari pubblici e privati della Route 53, il piano di controllo si trova nell' Regione AWS us-east-1 e i piani dati sono distribuiti a livello globale.

Amazon Route 53 si divide in piani di controllo e di dati nel seguente modo:

- Per il DNS pubblico e privato di Route 53, il piano di controllo è costituito dalla Route 53 APIs, che consente di gestire le voci DNS, inclusi sia Route 53 che Traffic Flow. APIs La console Route 53 si trova nella zona Regione AWS us-east-1, ma AWS se determina che c'è un problema in quella regione, la console Route 53 verrà servita da us-west-2. Regione AWS Il piano dei dati è il servizio DNS autoritativo, che funziona in oltre 200 punti di presenza (PoP) e che risponde alle query DNS basate sulle tue zone ospitate e sui dati di controllo dell'integrità.
- Per i controlli di integrità della Route 53, il piano di controllo è costituito dal Route 53 APIs che è possibile utilizzare per creare, aggiornare ed eliminare i controlli sanitari. La console per i controlli sanitari della Route 53 si trova nella zona Regione AWS us-east-1, ma AWS se si determina che c'è un problema in quella regione, la console per i controlli sanitari della Route 53 sarà servita da us-west-2. Regione AWS Il piano dati è il servizio distribuito globalmente, il quale realizza i controlli dell'integrità, raggruppa i risultati e li consegna ai piani dati dei DNS pubblici e privati di Route 53 e AWS Global Accelerator.
- Infatti Amazon Route 53 Resolver, il piano di controllo è costituito dal Route 53 Resolver APIs che consente di gestire le impostazioni di Amazon VPC, le regole Resolver, le politiche di registrazione delle query e le politiche del firewall DNS. Il piano dati è il servizio DNS resolver e risponde alle query DNS nel tuo VPC, agli endpoint che inoltrano le query verso altri resolver e al piano dati DNS Firewall che applica le policy di filtro delle query DNS. Resolver è un servizio regionale e i suoi piani di controllo e dati funzionano in modo indipendente in ciascuno di essi. Regione AWS
- Solo il piano di controllo in us-east-1 Regione AWS gestisce la registrazione del dominio nel Route 53.

Per ulteriori informazioni sui piani dati, sui piani di controllo e su come AWS crea servizi per soddisfare gli obiettivi di alta disponibilità, consulta il paper Static stability using Availability Zones nella Amazon Builders' Library.

Concetti sul controllo dell'integrità

Ecco una panoramica delle nozioni relative al controllo dell'integrità di Amazon Route 53.

- DNS failover
- endpoint

- health check

failover DNS

Un metodo per instradare il traffico lontano da risorse non integre e verso risorse integre. Quando si dispone di più di una risorsa che esegue la stessa funzione, ad esempio più di un server Web o un server di posta, è possibile configurare controlli dell'integrità di Route 53 per controllare l'integrità delle proprie risorse e configurare record nella zona ospitata per instradare il traffico solo verso le risorse integre.

Per ulteriori informazioni, consulta Configurazione di un failover DNS.

endpoint

La risorsa, ad esempio un server Web o un server di e-mail, per cui si configura un controllo dell'integrità. Puoi specificare un endpoint per IPv4 indirizzo (192.0.2.243), per indirizzo (2001:0 db 8:85 a IPv6 3:0000:0000:abcd: 0001:2345) o per nome di dominio (example.com).

> **Note**
>
> È inoltre possibile creare controlli sanitari che monitorino lo stato di altri controlli sanitari o che monitorino lo stato di allarme di un allarme. CloudWatch

controllo dell'integrità

Un componente di Route 53 che consente di eseguire le operazioni descritte di seguito.

- Monitorare se un endpoint specificato, ad esempio un server Web, è integro
- Facoltativamente, ricevere una notifica quando un endpoint diventa non integro
- Facoltativamente, configurare il failover DNS, che consente di reindirizzare il traffico Internet da una risorsa non integra a una risorsa integra

Per ulteriori informazioni su come creare e utilizzare i controlli dell'integrità, consulta Creazione di controlli sanitari su Amazon Route 53 .

Nozioni di base su Amazon Route 53

Per informazioni sulle operazioni di base relative ad Amazon Route 53, consulta gli argomenti seguenti in questa guida:

- Configura Amazon Route 53, che spiega come registrarsi AWS, come proteggere l'accesso al AWS proprio account e come configurare l'accesso programmatico a Route 53
- Nozioni di base su Amazon Route 53, che descrive come eseguire la registrazione di un nome di dominio, come creare un bucket Amazon S3 e configurarlo per l'hosting di siti Web statici e come instradare il traffico Internet al sito Web

Accesso a Amazon Route 53

Puoi accedere ad Amazon Route 53 nei seguenti modi:

- AWS Management Console— Le procedure contenute in questa guida spiegano come utilizzarlo AWS Management Console per eseguire attività.
- AWS SDKs— Se si utilizza un linguaggio di programmazione che AWS fornisce un SDK per, è possibile utilizzare un SDK per accedere a Route 53. SDKs semplifica l'autenticazione, si integra facilmente con il tuo ambiente di sviluppo e fornisci un facile accesso ai comandi di Route 53. Per ulteriori informazioni, consulta Strumenti per Amazon Web Services.
- API Route 53: se usi un linguaggio di programmazione per il quale non è disponibile un SDK, consulta la Documentazione di riferimento delle API di Amazon Route 53 per informazioni sulle operazioni API e su come effettuare richieste API.
- AWS Command Line Interface: per ulteriori informazioni, consulta Preparazione alla configurazione con AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface .
- AWS Tools for Windows PowerShell: per ulteriori informazioni, consulta Configurazione della AWS Tools for Windows PowerShell nella Guida per l'utente di AWS Tools for Windows PowerShell .

AWS Identity and Access Management

Amazon Route 53 si integra con AWS Identity and Access Management (IAM), un servizio che consente all'organizzazione di eseguire le seguenti operazioni:

- Crea utenti e gruppi con l'account della AWS tua organizzazione
- Condividi facilmente le risorse del tuo AWS account tra gli utenti dell'account
- Assegnare credenziali di sicurezza univoche a ciascun utente
- Controllare in modo granulare l'accesso dell'utente a servizi e risorse

Ad esempio, puoi utilizzare IAM con Route 53 per controllare quali utenti del tuo AWS account possono creare una nuova zona ospitata o modificare i record.

Per informazioni generali su IAM, consulta:

- Identity and Access Management in Amazon Route 53
- Identity and Access Management (IAM)
- Guida per l'utente di IAM

Prezzi e fatturazione di Amazon Route 53

Come per altri AWS prodotti, non ci sono contratti o impegni minimi per l'utilizzo di Amazon Route 53. Si paga solo per le zone ospitate configurate e il numero di query DNS a cui Route 53 risponde. Per ulteriori informazioni, consulta la pagina dei Prezzi Amazon Route 53.

Per informazioni sulla fatturazione AWS dei servizi, incluso come visualizzare la fattura e gestire l'account e i pagamenti, consulta la Guida per l'AWS Billing utente.

Utilizzo di Route 53 con un SDK AWS

AWS i kit di sviluppo software (SDKs) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK per Go	AWS SDK per Go esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice

Documentazione sugli SDK	Esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Strumenti per PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Per esempi specifici relativi a Route 53, consulta Esempi di codice per l'utilizzo di Route 53 AWS SDKs.

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Nozioni di base su Amazon Route 53

Inizia con le operazioni di base registrando un dominio con Amazon Route 53 e configurando Route 53 per rispondere alle query DNS che risolvono su in sito Web statico. Il primo tutorial ospita un sito Web statico in un bucket Amazon S3 aperto, mentre il secondo utilizza la CloudFront distribuzione Amazon per servire il sito Web con SSL/TLS.

Stima dei costi

- Vi è un costo annuale per registrare un dominio, che va da $9 a diverse centinaia di dollari, a seconda del dominio di primo livello, come .com. Per ulteriori informazioni, consulta Prezzi di Route 53 per la registrazione di un dominio. Questo costo non è rimborsabile.
- Quando record un dominio, creiamo automaticamente una zona ospitata pubblica con lo stesso nome del dominio. Puoi usare la zona ospitata per specificare dove desideri che Route 53 instradi il traffico per il tuo dominio.
- Durante questo tutorial, sarà creato un bucket Amazon S3 e sarà caricata una pagina Web di esempio. Se sei un nuovo AWS cliente, puoi iniziare a usare Amazon S3 gratuitamente. Se sei un AWS cliente esistente, gli addebiti si basano sulla quantità di dati archiviati, sul numero di richieste di dati e sulla quantità di dati trasferiti. Per ulteriori informazioni, consulta Prezzi di Amazon S3.
- CloudFront le tariffe si basano sul numero di richieste di dati, sul numero di edge location utilizzate e sulla quantità di dati trasferiti. Per ulteriori informazioni, consulta CloudFront Prezzi.

Argomenti

Configura Amazon Route 53

La panoramica e le procedure in questa sezione ti aiutano a iniziare AWS.

Argomenti

- Download degli strumenti

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Download degli strumenti

AWS Management Console Include una console per Amazon Route 53, ma se desideri accedere ai servizi in modo programmatico, consulta quanto segue:

- La guida API indica le operazioni supportate dai servizi e fornisce collegamenti alla relativa documentazione SDK e CLI:
  - Documentazione di riferimento API di Amazon Route 53
- Per chiamare un'API senza dover gestire dettagli di basso livello come l'assemblaggio di richieste HTTP non elaborate, puoi utilizzare un SDK. AWS AWS SDKs Forniscono funzioni e tipi di dati che incapsulano la funzionalità dei servizi. AWS Per scaricare un AWS SDK e accedere alle istruzioni di installazione, consulta la pagina pertinente:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Per un elenco completo di AWS SDKs, consulta Tools for Amazon Web Services.
- Puoi usare il AWS Command Line Interface (AWS CLI) per controllare più AWS servizi dalla riga di comando. È inoltre possibile automatizzare i comandi utilizzando gli script. Per ulteriori informazioni, consulta AWS Command Line Interface.
- AWS Tools for Windows PowerShell supporta questi AWS servizi. Per ulteriori informazioni, consulta la Documentazione di riferimento per Cmdlet AWS Strumenti per PowerShell.

Utilizzo del proprio dominio per un sito Web statico in un bucket Amazon S3

Questo tutorial sulle operazioni di base illustra come completare le seguenti attività:

- Registrare un nome di dominio, come esempio.com
- Creazione di un bucket Amazon S3 e configurazione per l'hosting di un sito Web

- Creare un sito Web di esempio e salvare il file nel bucket S3
- Configurazione di Amazon Route 53 per instradare il traffico verso il nuovo sito Web

Una volta terminato, sarai in grado di aprire un browser, immettere il nome di dominio e visualizzare il tuo sito Web.

> **Note**
>
> Puoi anche trasferire un dominio esistente a Route 53, ma il processo è più complesso e dispendioso in termini di tempo rispetto alla registrazione di un nuovo dominio. Per ulteriori informazioni, consulta Trasferimento della registrazione per un dominio ad Amazon Route 53.

Argomenti

Prerequisiti

Prima di iniziare, devi accertarti di aver completato le fasi in Configura Amazon Route 53.

Fase 1: registrare un dominio

Per utilizzare un nome di dominio come esempio.com, devi trovare un nome di dominio che non sia già in uso e registrarlo. Quando record un nome di dominio, lo prenoti per il tuo uso esclusivo ovunque su Internet, in genere per un anno. Per impostazione predefinita, rinnoveremo automaticamente il tuo nome di dominio al termine di ogni anno, ma potrai disabilitare il rinnovo automatico. Per ulteriori informazioni, consulta Registrazione di un nuovo dominio.

Fase 2: Creazione di un bucket S3 per il dominio root

Amazon S3 consente di archiviare e recuperare i tuoi dati da qualsiasi luogo tramite Internet. Per organizzare i dati, devi creare bucket e caricare i dati per il bucket utilizzando la AWS Management Console. Puoi utilizzare Amazon S3 S3 per ospitare un sito Web statico in un bucket. Nella procedura seguente viene descritto come creare un bucket.

Come creare un bucket S3 per il dominio root

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona Crea bucket.
3. Immetti uno dei seguenti valori:

   Nome bucket

   Digita il nome del dominio, ad esempio example.com.

   Regione

   Scegli la regione più vicina alla maggior parte dei tuoi utenti.

   Prendi nota della regione che scegli; avrai bisogno di queste informazioni più tardi nel processo.
4. Per accettare le impostazioni di default e creare il bucket, scegli Crea bucket.

Fase 3 (facoltativa): Creazione di un altro bucket S3 per il tuo sottodominio

Nella procedura precedente, hai creato un bucket per il tuo nome di dominio, ad esempio esempio.com. In questo modo gli utenti possono accedere al tuo sito web utilizzando il tuo nome di dominio, ad esempio esempio.com.

Se desideri che anche i tuoi utenti possano utilizzare www. *your-domain-name*, ad esempio www.example.com, per accedere al tuo sito web di esempio, crea un secondo bucket S3. Configura il secondo bucket per instradare il traffico verso il primo bucket.

Per creare un bucket S3 per www. your-domain-name

1. Seleziona Crea bucket.
2. Immetti uno dei seguenti valori:

   Nome bucket

   Inserisci www. ***your-domain-name***. Ad esempio, se hai registrato il nome di dominio esempio.com, immetti www.esempio.com.

   Regione

   Scegli la stessa regione in cui hai creato il primo bucket.
3. Per accettare le impostazioni predefinite e creare il bucket, scegliere Create (Crea).

Fase 4: Configurazione di un bucket del dominio root per l'hosting di siti Web

Ora che hai un bucket S3, puoi configurarlo per l'hosting di siti Web.

Come consentire l'hosting di siti Web sul bucket S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nell'elenco Bucket, seleziona il nome del bucket per cui desideri abilitare l'hosting di siti Web statici.
3. Scegli Properties (Proprietà).
4. In Hosting di siti Web statici, seleziona Abilita.
5. Seleziona Utilizza questo bucket per l'hosting di un sito Web.
6. In Hosting di siti Web statici, seleziona Abilita.
7. In Documento di indice immettere il nome file del documento di indice, in genere `index.html`.

   Il nome del documento indice fa distinzione tra maiuscole e minuscole e deve corrispondere esattamente al nome del file del documento indice HTML che si prevede di caricare nel bucket S3. Quando si configura un bucket per l'hosting di siti Web, è necessario specificare un

documento di indice. Amazon S3 restituisce questo documento di indice quando si eseguono richieste per il dominio root o per una delle sottocartelle.

8. (Facoltativo) Se desideri fornire il tuo documento di errore personalizzato per gli errori di classe 4XX, in Documento di errore, specifica il nome del file del documento di errore personalizzato.

   Se non si specifica un documento di errore personalizzato e si verifica un errore, Amazon S3 restituisce un documento di errore HTML predefinito.

9. (Facoltativo) Per specificare regole di reindirizzamento avanzate, in Regole reindirizzamento, utilizza XML per descrivere le regole.

   Per ulteriori informazioni, consulta Configurazione dei reindirizzamenti condizionali avanzati nella Guida per l'utente Amazon Simple Storage Service.

10. Scegli Save changes (Salva modifiche).
11. In Hosting sito Web statico, prendi nota dell'endpoint.

    Endpoint è l'endpoint del sito web Amazon S3 per il bucket. Dopo aver configurato il bucket come sito Web statico, sarà possibile utilizzare questo endpoint per testare il sito Web, come riportato in Fase 9: test dell'endpoint del dominio.

    Dopo aver completato le seguenti fasi per modificare le impostazioni per l'accesso pubblico e aver aggiunto una policy del bucket che consente l'accesso pubblico in lettura, potrai utilizzare l'endpoint del sito Web per accedere al sito Web.

Fase 5: (facoltativa): Configurazione del bucket del sottodominio per il reindirizzamento del sito Web

Una volta che il bucket del dominio root è stato configurato per l'hosting di siti Web, è possibile configurare il bucket del sottodominio per reindirizzare tutte le richieste al dominio root. Ad esempio, è possibile configurare tutte le richieste per `www.example.com` per essere reindirizzato a `example.com`.

Come configurare un reindirizzamento

1. Nella console Amazon S3, nell'elenco Bucket, seleziona il bucket del sottodominio (in questo esempio, `www.example.com`).
2. Scegliere Properties (Proprietà).
3. In Hosting di siti Web statici, seleziona Modifica.

4. Seleziona Reindirizza richieste per un oggetto.
5. Nella casella Target bucket (Bucket di destinazione) immettere il dominio root, ad esempio, **`example.com`**.
6. In Protocol (Protocollo), scegliere HTTP.
7. Scegli Save changes (Salva modifiche).

Fase 6: Caricamento dell'indice per creare i contenuti di un sito Web

Quando si abilita l'hosting di siti Web statici per il bucket, si immette il nome del documento di indice (ad esempio, **`index.html`**). Dopo aver abilitato l'hosting di siti Web statici per il bucket, carica un file HTML con il nome del documento di indice nel bucket.

Come caricare un file indice

1. Copia il seguente testo di esempio che è possibile utilizzare come sito Web semplice di una sola pagina per questo tutorial, incollalo in un editor di testo e salvalo come 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. Nell'elenco Nome bucket, seleziona il nome del bucket per cui desideri abilitare l'hosting di siti Web statici.
3. Nella console Amazon S3 scegli il nome del bucket creato nella procedura Come consentire l'hosting di siti Web sul bucket S3 (fai clic sul nome del bucket collegato).

4. Scegli Carica, Aggiungi file, seleziona index.html dalla posizione in cui è stato salvato, quindi seleziona Carica.
5. Se hai creato un documento di errore, ad esempio, **`404.html`**per caricarlo, completa le fasi da 3 a 5.

Fase 7: modifica delle impostazioni dell'accesso pubblico ai blocchi Amazon S3

Per impostazione predefinita, Amazon S3 blocca l'accesso pubblico all'account e ai bucket. Per utilizzare un bucket per ospitare un sito Web statico, puoi seguire questa procedura per modificare le impostazioni di blocco dell'accesso pubblico.

> **Warning**
>
> Prima di completare questa fase, esamina Blocco dell'accesso pubblico all'archiviazione Amazon S3 per essere certo di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

Per instradare il traffico verso il tuo sito Web

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona il nome del bucket configurato come sito Web statico.
3. Seleziona Autorizzazioni.
4. In Blocca accesso pubblico (impostazioni bucket), seleziona Modifica.
5. Deseleziona Blocca tutto l'accesso pubblico, quindi seleziona Salva modifiche.

Amazon S3 disattiva le impostazioni di blocco dell'accesso pubblico per il tuo bucket. Per creare un sito web pubblico statico, potrebbe essere necessario modificare anche le impostazioni di blocco dell'accesso pubblico per l'account prima di aggiungere una policy del bucket. Se le impostazioni dell'account per il blocco dell'accesso pubblico sono attualmente attivate, verrà visualizzata una nota in Blocca accesso pubblico (impostazioni bucket).

Fase 8: collegare una policy del bucket

Dopo aver modificato le impostazioni di blocco dell'accesso pubblico Amazon S3, è possibile aggiungere una policy del bucket per concedere l'accesso pubblico in lettura agli oggetti nel bucket. Quando concedi l'accesso pubblico in lettura, chiunque su Internet può accedere al bucket.

> **Warning**
>
> Prima di completare questa fase, esamina Blocco dell'accesso pubblico all'archiviazione Amazon S3 per essere certo di aver compreso e accettato i rischi connessi alla concessione dell'accesso pubblico. Quando si disattivano le impostazioni di blocco dell'accesso pubblico per rendere pubblico il bucket, chiunque su Internet può accedere al bucket. Consigliamo di bloccare tutti gli accessi pubblici ai bucket.

Per instradare il traffico verso il tuo sito Web

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. In Bucket, scegli il nome del bucket.
3. Seleziona Autorizzazioni.
4. In Policy del bucket, seleziona Modifica.
5. Copia la seguente policy bucket e incollala in un editor di testo. Questa policy concede a tutti gli utenti su Internet (`"Principal":"*"`) l'autorizzazione per ottenere i file (`"Action":["s3:GetObject"]`) nel bucket S3 che è associato al tuo nome di dominio (`"arn:aws:s3:::`*`your-domain-name`*`/*"`).

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

```
}
```

6. Aggiorna il valore di `Resource` to*your-domain-name*, ad esempio**example.com**.
7. Scegli Save changes (Salva modifiche).

Fase 9: test dell'endpoint del dominio

Dopo aver configurato il bucket di dominio per ospitare un sito Web pubblico, puoi testare l'endpoint. Sarai in grado di testare l'endpoint per il bucket di dominio, poiché il bucket del sottodominio è impostato per il reindirizzamento del sito Web e non per l'hosting statico del sito Web.

> **Note**
>
> Amazon S3 non supporta l'accesso HTTPS al sito web. Se desideri utilizzare HTTPS, puoi utilizzare Amazon CloudFront per servire un sito Web statico ospitato su Amazon S3.
> Per ulteriori informazioni, consulta Richiedere HTTPS per la comunicazione tra gli spettatori e. CloudFront

1. In Bucket, scegli il nome del bucket.
2. Scegliere Properties (Proprietà).
3. Nella parte inferiore della pagina, in Static website hosting (Hosting di siti Web statici), scegliere il proprio Bucket website endpoint (Endpoint del sito web Bucket).

   Il documento indice viene aperto in una finestra del browser separata.

Fase 10: Instradamento del traffico DNS per il dominio al bucket del sito Web

Nel tuo bucket S3 disponi ora di un sito Web di una pagina. Per iniziare a instradare il traffico Internet per il tuo dominio al tuo bucket S3, esegui la procedura seguente.

Per instradare il traffico verso il tuo sito Web

1. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.

> **Note**
>
> Quando hai registrato il tuo dominio, Amazon Route 53 ha creato automaticamente una zona ospitata con lo stesso nome. Una zona ospitata contiene informazioni su come desideri che Route 53 instradi il traffico per il dominio.

3. Nell'elenco delle zone ospitate, scegli il nome del dominio.
4. Scegli Crea record.

> **Note**
>
> Ciascun record contiene informazioni relative alle modalità con cui desideri instradare il traffico su Internet per un dominio (come esempio.com) o un sottodominio (come www.esempio.com o test.esempio.com). I record vengono memorizzati nella zona ospitata per il tuo dominio.

5. Seleziona Passa alla procedura guidata.
6. Scegli Routing semplice, quindi Successivo.
7. Scegli Define simple record (Definisci record semplice).
8. In Record name (Nome del record) accetta il valore predefinito, che è il nome della zona ospitata e del dominio.
9. In Tipo di record, scegli A - Indirizza il traffico verso un IPv4 indirizzo e alcune AWS risorse.
10. In Value/Route traffic to (Valore/Instradamento traffico a), seleziona Alias to S3 website endpoint (Alias all'endpoint del sito Web S3).
11. Scegli la regione.
12. Scegli il bucket S3.

    Il nome del bucket deve corrispondere al nome visualizzato nella casella Name (Nome). Nell'elenco Scegli bucket S3, il nome del bucket viene visualizzato con l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio, `s3-website-us-west-1.amazonaws.com (example.com)`.

    Scegli il bucket S3 riporta un bucket se una delle seguenti condizioni è vera:

    - Hai configurato il bucket come sito Web statico.
    - Il nome del bucket è uguale al nome del record che stai creando.

- L' AWS account corrente ha creato il bucket.

Se il bucket non viene visualizzato nell'elenco Scegli bucket S3, specifica l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio **`s3-website-us-west-2.amazonaws.com`**. Per un elenco completo degli endpoint dei siti Web Amazon S3, consulta Endpoint di siti Web Amazon S3. Per ulteriori informazioni sulla destinazione alias, consulta la sezione "Valore/instradamento traffico a" nella Valori specifici per record alias semplici.

13. Per Evaluate target health (Valuta integrità target), seleziona No.
14. Scegli Define simple record (Definisci record semplice).

(Facoltativo) Come aggiungere un record alias al sottodominio (**`www.example.com`**)

Se hai creato un bucket per il tuo sottodominio, aggiungi anche un record alias.

1. In Configura record, seleziona Definisci record semplice.
2. In Record name (Nome del record) per il sottodominio digita `www`.
3. In Tipo di record, scegli A - Indirizza il traffico verso un IPv4 indirizzo e alcune AWS risorse.
4. In Value/Route traffic to (Valore/Instradamento traffico a), seleziona Alias to S3 website endpoint (Alias all'endpoint del sito Web S3).
5. Scegli la regione.
6. Seleziona il bucket S3, ad esempi, `s3-website-us-west-2.amazonaws.com (example.com)`.

   Se il bucket non viene visualizzato nell'elenco Scegli bucket S3, specifica l'endpoint del sito Web di Amazon S3 per la regione in cui è stato creato il bucket, ad esempio **`s3-website-us-west-2.amazonaws.com`**.
7. Per Evaluate target health (Valuta integrità target), seleziona No.
8. Scegli Define simple record (Definisci record semplice).
9. Nella pagina Configura record, scegli Crea record.

Fase 11: Test del sito Web

Per verificare che il sito Web funzioni correttamente, aprite un browser Web e accedete a quanto segue URLs:

- http://*your-domain-name*, ad esempio, `example.com` — Visualizza il documento indice nel *your-domain-name* bucket
- http://www. *your-domain-name*ad esempio, `www.example.com` — Reindirizza la tua richiesta al bucket *your-domain-name*

In alcuni casi può essere necessario pulire la cache per osservare il comportamento previsto.

Per informazioni avanzate su come instradare il traffico Internet, consulta Configurazione di Amazon Route 53 come servizio DNS. Per informazioni su come indirizzare il traffico Internet verso le risorse, consulta. AWS Instradamento del traffico Internet verso le tue risorse AWS

Passaggio 12 (opzionale): usa Amazon CloudFront per accelerare la distribuzione dei tuoi contenuti

CloudFront è un servizio web che velocizza la distribuzione di contenuti web statici e dinamici, come .html, .css, .js e file di immagine, agli utenti. CloudFront distribuisce i tuoi contenuti attraverso una rete mondiale di data center denominati edge location. Quando un utente richiede i contenuti che utilizzi CloudFront, viene indirizzato verso l'edge location che offre la latenza (ritardo) più bassa, in modo che i contenuti vengano forniti con le migliori prestazioni possibili.

- Se il contenuto si trova già nell'edge location con la latenza più bassa, lo CloudFront consegna immediatamente.
- Se il contenuto non si trova in quella edge location, lo CloudFront recupera da un bucket Amazon S3 o da un server HTTP (ad esempio un server Web) che hai identificato come origine per la versione definitiva dei tuoi contenuti.

Per informazioni sull'utilizzo CloudFront per distribuire i contenuti nel tuo bucket Amazon S3, consulta Aggiungere CloudFront quando distribuisci contenuti da Amazon S3 nella Amazon Developer Guide. CloudFront

Usa una CloudFront distribuzione Amazon per servire un sito Web statico

Questo tutorial sulle operazioni di base illustra come completare le seguenti attività:

- Registra un nome di dominio, come esempio.com.
- Crea un certificato per il dominio.
- Crea due bucket Amazon S3 e configurane uno per ospitare un sito Web e l'altro per reindirizzare al sottodominio.
- Crea un sito Web di esempio e salva il file nel bucket S3.
- Crea CloudFront distribuzioni per entrambi i bucket S3.
- Configura Amazon Route 53 per indirizzare il traffico verso le CloudFront distribuzioni.

Una volta terminato, sarai in grado di aprire un browser, immettere il nome di dominio e visualizzare il tuo sito Web in maniera sicura.

Argomenti

Prerequisiti

Prima di iniziare, devi accertarti di aver completato le fasi in Configura Amazon Route 53.

Fase 1: registrare un dominio

Per utilizzare un nome di dominio come esempio.com, devi trovare un nome di dominio che non sia già in uso e registrarlo. Quando record un nome di dominio, lo prenoti per il tuo uso esclusivo ovunque su Internet, in genere per un anno. Per impostazione predefinita, rinnoveremo automaticamente il tuo nome di dominio al termine di ogni anno, ma potrai disabilitare il rinnovo automatico. Per ulteriori informazioni, consulta Registrazione di un nuovo dominio.

Fase 2: Richiesta di un certificato pubblico

È necessario un certificato pubblico per configurare CloudFront CloudFront le distribuzioni Amazon in modo da richiedere che gli spettatori utilizzino HTTPS in modo che le connessioni siano crittografate quando CloudFront comunicano con gli spettatori.

Per richiedere un certificato pubblico AWS Certificate Manager(ACM) (console)

1. Accedi alla console di AWS gestione e apri la console ACM da casahttps://console.aws.amazon.com/acm/.

   > **Note**
   >
   > Assicurati di creare il certificato nella regione Stati Uniti orientali (Virginia settentrionale). Questo è obbligatorio per Amazon CloudFront.

   Nella riquadro di navigazione a sinistra seleziona Richiedi un certificato e alla voce Richiedi pagina certificato seleziona Richiedi un certificato pubblico, quindi vai su Seguente.
2. Nella sezione Nomi dominio inserisci il dominio, ad esempio **`example.com`**.

   Seleziona Aggiungi un altro nome a questo certificato, inserisci un asterisco davanti al nome di dominio per richiedere un certificato con caratteri jolly per tutti i sottodomini, ad esempio **`*.example.com`**.
3. Nella sezione Seleziona metodo di convalida seleziona Convalida DNS.
4. Nella sezione Algoritmo chiave, seleziona RSA 2048.
5. Nella sezione Aggiungi tag, se lo desideri, puoi taggare il certificato. I tag sono coppie chiave-valore che fungono da metadati per identificare e organizzare le risorse. AWS

   Seleziona Richiedi per farsi indirizzare alla pagina Certificati.

6. Quando lo stato del nuovo certificato appare In sospeso, scegli l'ID del certificato e nella pagina dei dettagli del certificato seleziona Crea record in Route 53 in modo da aggiungere automaticamente i record CNAME per i domini, quindi seleziona Crea record.

   La pagina Certificate status (Stato del certificato) dovrebbe essere aperta con un banner di stato che visualizza Successfully created DNS records (Registri DNS creati con successo).

   Il nuovo certificato potrebbe ancora visualizzare lo stato Pending validation (Convalida in attesa) per un massimo di 30 minuti.

Fase 3: Creazione di un bucket S3 per l'hosting del sottodominio

Per creare un bucket S3 per www. your-domain-name

Amazon S3 consente di archiviare e recuperare i tuoi dati da qualsiasi luogo tramite Internet. In questa fase viene creato un bucket S3 per archiviare tutti i file per il sito Web.

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona Crea bucket.
3. Immetti uno dei seguenti valori:

   Nome bucket

   Inserisci www. ***your-domain-name***. Ad esempio, se hai registrato il nome di dominio esempio.com, immetti www.esempio.com.

   Regione

   Scegli una regione per il bucket.
4. Per accettare le impostazioni di default e creare il bucket, scegli Crea bucket.

   Per ulteriori informazioni sulle impostazioni del bucket S3, consulta Visualizza proprietà del bucket nella Guida per l'utente di Amazon S3.

Fase 4: Creazione di un altro bucket S3 per il dominio root

Se desideri che anche i tuoi utenti siano in grado di utilizzare il dominio root,. *your-domain-name*(ad esempio example.com) per accedere al tuo sito web di esempio, crea un secondo bucket

S3. In questo tutorial dovrai quindi configurare il secondo bucket (dominio root) per instradare il traffico verso il primo bucket.

Per creare un bucket S3 per your-domain-name

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Seleziona Crea bucket.
3. Immetti uno dei seguenti valori:

   Nome bucket

   Specificare ***your-domain-name***. Ad esempio, se hai registrato il nome di dominio esempio.com, immetti esempio.com.

   Regione

   Scegli la stessa regione in cui hai creato il primo bucket.
4. Per accettare le impostazioni di default e creare il bucket, scegli Crea bucket.

Fase 5: Caricamento dei file del sito Web nel tuo bucket di sottodominio

Ora che hai un bucket S3, puoi caricare i file del tuo sito Web. In questo tutorial dovrai caricare un semplice file index.html che visualizza il testo su una pagina.

Come abilitare il bucket S3 per l'hosting di siti Web

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nell'elenco Bucket seleziona il nome collegato del bucket in cui desideri caricare i file del sito Web, ad esempio **www.example.com**.
3. Copia il testo di esempio che crea un sito Web semplice di una pagina, incollalo in un editor di testo e salvalo come 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. Nella scheda Oggetti, scegli Carica.
5. In Cartelle e file, scegli Aggiungi file e carica i file del tuo sito Web. Per questo tutorial, carica il file index.html salvato nel passaggio 3 di questa procedura.

Fase 6: Configurazione del bucket del dominio root per il reindirizzamento del sito Web

Una volta che il bucket del dominio root è stato configurato per l'hosting di siti Web, è possibile configurare il bucket del dominio root per reindirizzare tutte le richieste al sottodominio. Ad esempio, è possibile configurare tutte le richieste per `example.com` per essere reindirizzato a `www.example.com`.

Come configurare un reindirizzamento

1. Nella console Amazon S3, nell'elenco Bucket, seleziona il nome del bucket (in questo esempio, `example.com`).
2. Scegliere Properties (Proprietà).
3. In Hosting di siti Web statici, seleziona Modifica.
4. In Hosting di siti Web statici, seleziona Abilita.
5. Seleziona Reindirizza richieste per un oggetto.
6. Nella casella Nome host specifica il sottodominio, ad esempio **`www.example.com`**.
7. In Protocol (Protocollo), scegli HTTPS.
8. Scegli Save changes (Salva modifiche).
9. In Hosting sito Web statico, prendi nota dell'endpoint.

Endpoint è l'endpoint del sito web Amazon S3 per il bucket. Utilizzerai questo endpoint per configurare una CloudFront distribuzione Amazon.

Passaggio 7: crea una CloudFront distribuzione Amazon per il tuo sottodominio

In questa fase crei una distribuzione CloudFront per il tuo sottodominio, ad esempio www.esempio.com, per consentire al tuo sito web di utilizzare HTTPS in modo che le persone possano visualizzarlo in modo sicuro.

Per creare una distribuzione CloudFront

1. Apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.
2. Scegliere Create Distribution (Crea distribuzione).
3. Sotto la voce Origine, per Dominio origine scegli il bucket Amazon S3 creato in precedenza. Il formato sarà simile a**`www.example.com.s3.<Region>.amazonaws.com`**.

   Per Accesso origine, seleziona Identità di accesso legacy. Per Identità di accesso origine, puoi scegliere dall'elenco o selezionare Crea un nuovo OAI(funzionano entrambe le opzioni).

   In Policy del bucket, scegli Sì, aggiorna la policy del bucket.
4. Per le impostazioni in Impostazioni predefinite del comportamento della cache, in Viewer (Visualizzatore), imposta Viewer protocol policy (Policy protocollo visualizzatore) su Redirect HTTP to HTTPS (Reindirizza da HTTP a HTTPS) e accetta i valori predefiniti rimanenti.

   Per ulteriori informazioni sulle opzioni di comportamento della cache, consulta le impostazioni del comportamento della cache nella guida per CloudFront sviluppatori di Amazon.
5. Nella sezione Web Application Firewall (WAF) puoi stabilire se abilitare o disabilitare le protezioni di sicurezza AWS WAF .
6. In Impostazioni, procedi come segue:

   - Scegli Aggiungi elemento per Nome di dominio alternativo (CNAME) - facoltativo, quindi inserisci il tuo sottodominio, ad esempio **`www.example.com`**.
   - Per Certificato SSL personalizzato, scegli il certificato creato in precedenza.
   - Nella casella di testo Oggetti root di default, digita **`index.html`**.
   - Per il resto, accetta i valori predefiniti e scegli Crea distribuzione.

Per ulteriori informazioni sulle opzioni di distribuzione, consulta Impostazioni distribuzione.

7. Dopo aver CloudFront creato la distribuzione, il valore della colonna Status relativa alla distribuzione cambia da In corso a Deployed. In genere sono necessari pochi minuti.

   Registra il nome di dominio CloudFront assegnato alla tua distribuzione, che appare nell'elenco delle distribuzioni. Puoi utilizzare questo nome di dominio per testare la distribuzione.

Passaggio 8: crea una CloudFront distribuzione Amazon per il tuo dominio principale

In questo passaggio crei una CloudFront distribuzione per il tuo dominio root in modo che utilizzi HTTPS quando il relativo URL viene reindirizzato al sottodominio.

Per creare una distribuzione CloudFront

1. Apri la CloudFront console all'indirizzo. https://console.aws.amazon.com/cloudfront/v4/home
2. Scegliere Create Distribution (Crea distribuzione).
3. In Impostazioni di origine, per Nome dominio origine, specifica l'endpoint del sito Web del bucket. Questo valore viene ottenuto dalla sezione Hosting del sito Web statico di Proprietà per il bucket Amazon S3 creato in precedenza.

   Per il resto, accetta i valori di default.
4. Nella sezione Web Application Firewall (WAF) puoi stabilire se abilitare o disabilitare le protezioni di sicurezza AWS WAF .
5. Per i campi sotto la chiave di cache e le richieste di origine, scegli Cache policy e origin requests policy (consigliato) e nel menu a discesa Cache policy, scegli CachingDisabled

   Per il resto, accetta i valori di default.

   Per ulteriori informazioni sulle opzioni di comportamento della cache, consulta le impostazioni del comportamento della cache nella guida per CloudFront sviluppatori di Amazon.
6. In Impostazioni, procedi come segue:

   - Scegli Aggiungi elemento per Nome di dominio alternativo (CNAME) - facoltativo, quindi inserisci il tuo dominio root, ad esempio **`example.com`**.

- Per Certificato SSL personalizzato, scegli il certificato creato in precedenza.
- Per il resto, accetta i valori di default.

Per ulteriori informazioni sulle opzioni di distribuzione, consulta Impostazioni distribuzione.

7. Nella parte inferiore della pagina, seleziona Crea previsione.
8. Dopo aver CloudFront creato la distribuzione, il valore della colonna Status relativa alla distribuzione cambia da In corso a Deployed. In genere sono necessari pochi minuti.

   Registra il nome di dominio CloudFront assegnato alla tua distribuzione, che appare nell'elenco delle distribuzioni. È possibile utilizzare questo nome di dominio per testare la distribuzione,

Passaggio 9: instradamento del traffico DNS per il tuo dominio nella distribuzione CloudFront

Ora hai un sito web di una pagina nel tuo bucket S3 che utilizza una distribuzione. CloudFront Per iniziare a indirizzare il traffico Internet dal tuo dominio alla CloudFront distribuzione, esegui la procedura seguente.

Per ulteriori informazioni sull'instradamento del traffico verso le CloudFront distribuzioni, consulta. Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio

Per instradare il traffico verso il tuo sito Web

1. Apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.

   > **Note**
   >
   > Quando hai registrato il tuo dominio, Amazon Route 53 ha creato automaticamente una zona ospitata con lo stesso nome. Una zona ospitata contiene informazioni su come desideri che Route 53 instradi il traffico per il dominio.

3. Nell'elenco delle zone ospitate, scegli il nome del dominio.
4. Scegli Crea record.

Se ti trovi nella vista Creazione rapida del record, scegli Passa alla procedura guidata.

> **Note**
>
> Ciascun record contiene informazioni relative alle modalità con cui desideri instradare il traffico su Internet per un dominio (come esempio.com) o un sottodominio (come www.esempio.com o test.esempio.com). I record vengono memorizzati nella zona ospitata per il tuo dominio.

5. Scegli Routing semplice, quindi Successivo.
6. Scegli Define simple record (Definisci record semplice).
7. In Nome del record digita **`www`** davanti al valore di default, che è il nome della zona ospitata e del dominio.
8. In Tipo di record, scegli A - Indirizza il traffico verso un IPv4 indirizzo e alcune AWS risorse.
9. In Value/Indirizza il traffico verso, scegli Alias alla distribuzione. CloudFront
10. Scegli la distribuzione.

    Il nome della distribuzione deve corrispondere al nome visualizzato nella casella Nome dominio nell'elenco Distribuzioni, ad esempio `dddjjjkkk.cloudfront.net`.
11. Per Evaluate target health (Valuta integrità target), seleziona No.
12. Scegli Define simple record (Definisci record semplice).

Per aggiungere un record di alias al dominio root (**`example.com`**)

Aggiungi un record alias per il dominio root, in modo che punti al bucket S3 che reindirizza il traffico a `www.example.com`. Per ulteriori informazioni sull'instradamento del traffico verso le distribuzioni, consulta CloudFront . Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio

1. Nel pannello di navigazione, scegli Zone ospitate.
2. Nell'elenco delle zone ospitate, scegli il nome del dominio.
3. Scegli Crea record.

   Se ti trovi nella vista Creazione rapida del record, scegli Passa alla procedura guidata.

> **Note**
>
> Ciascun record contiene informazioni relative alle modalità con cui desideri instradare il traffico su Internet per un dominio (come esempio.com) o un sottodominio (come www.esempio.com o test.esempio.com). I record vengono memorizzati nella zona ospitata per il tuo dominio.

4. Scegli Routing semplice, quindi Successivo.
5. Scegli Define simple record (Definisci record semplice).
6. In Nome record accetta il valore di default.
7. In Tipo di record, scegli A - Indirizza il traffico verso un IPv4 indirizzo e alcune AWS risorse.
8. In Valore/instradamento traffico in, scegli Distribuzione da alias a CloudFront .
9. Scegli la distribuzione.

   Il nome della distribuzione deve corrispondere al nome visualizzato nella casella Nome dominio nell'elenco Distribuzioni, ad esempio `dddjjjkkk.cloudfront.net`.
10. Per Evaluate target health (Valuta integrità target), seleziona No.
11. Scegli Define simple record (Definisci record semplice).
12. Nella pagina Configura record, scegli Crea record.

Fase 10: Test del sito Web

Per verificare che il sito Web funzioni correttamente, aprite un browser Web e accedete a quanto segue URLs:

- https://www. *`your-domain-name`*, ad esempio, `www.example.com` — Visualizza il documento indice nel *`www.your-domain-name`* bucket
- https://ad *`your-domain-name`* esempio, `example.com` — Reindirizza la richiesta al bucket *`www.your-domain-name`*

In alcuni casi può essere necessario pulire la cache per osservare il comportamento previsto.

Per informazioni avanzate su come instradare il traffico Internet, consulta Configurazione di Amazon Route 53 come servizio DNS. Per informazioni su come indirizzare il traffico Internet verso le risorse, consulta. AWS Instradamento del traffico Internet verso le tue risorse AWS

Integrazione con altri servizi

Puoi integrare Amazon Route 53 con altri AWS servizi per registrare le richieste inviate all'API Route 53, monitorare lo stato delle risorse e assegnare tag alle risorse. Puoi anche utilizzare Route 53 per instradare il traffico Internet alle tue risorse AWS .

Argomenti

Logging, monitoraggio e tagging

AWS CloudTrail

Amazon Route 53 è integrato con AWS CloudTrail, un servizio che acquisisce informazioni su ogni richiesta inviata all'API Route 53 dal tuo AWS account. Puoi utilizzare le informazioni contenute nei file di CloudTrail registro per determinare quali richieste sono state fatte a Route 53, l'indirizzo IP di origine da cui è stata effettuata ogni richiesta, chi ha effettuato la richiesta, quando è stata effettuata e così via.

Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon Route 53 con AWS CloudTrail.

Amazon CloudWatch

Puoi utilizzare Amazon CloudWatch per monitorare lo stato, integro o meno, dei tuoi controlli sanitari sulla Route 53. I controlli dell'integrità monitorano lo stato e le prestazioni delle applicazioni Web, dei server Web e di altre risorse. A intervalli regolari specificati, Route 53 inoltra le richieste automatizzate tramite Internet alla tua applicazione, server o altre risorse per verificare che sia raggiungibile, disponibile e funzionante.

Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

Editor di tag

Un tag è un'etichetta che assegni a una AWS risorsa, inclusi i domini Route 53, le zone ospitate e i controlli sanitari. Ogni tag consiste di una chiave e di un valore, entrambi personalizzabili. Ad esempio, puoi assegnare un tag alla registrazione di un dominio che dispone della chiave

"Customer" e del valore "Example Corp." È possibile utilizzare i tag per diversi scopi; uno degli usi più comuni è quello di classificare e tenere traccia dei costi. AWS

Per ulteriori informazioni, consulta Assegnazione di tag alle risorse di Amazon Route 53.

Instradamento del traffico verso altre risorse AWS

Puoi utilizzare Amazon Route 53 per indirizzare il traffico verso una varietà di AWS risorse.

Amazon API Gateway

Amazon API Gateway ti consente di creare, pubblicare, gestire, monitorare e proteggere APIs su qualsiasi scala. Puoi creare APIs quell'accesso AWS o altri servizi web, oltre ai dati archiviati nel AWS cloud.

Route 53 può essere utilizzato per instradare il traffico a un'API di API Gateway. Per ulteriori informazioni, consulta Routing del traffico a un'API di Amazon API Gateway usando il proprio nome di dominio.

Amazon CloudFront

Per velocizzare la distribuzione dei tuoi contenuti web, puoi utilizzare Amazon CloudFront, la rete di distribuzione AWS dei contenuti (CDN). CloudFront è in grado di distribuire l'intero sito Web, inclusi contenuti dinamici, statici, in streaming e interattivi, utilizzando una rete globale di edge location. CloudFront indirizza le richieste di contenuti verso l'edge location che offre agli utenti la latenza più bassa. Puoi utilizzare Route 53 per indirizzare il traffico dal tuo dominio alla tua CloudFront distribuzione. Per ulteriori informazioni, consulta Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio.

Amazon EC2

Amazon EC2 offre capacità di elaborazione scalabile nel AWS cloud. Puoi avviare un ambiente di elaborazione EC2 virtuale (un'istanza) utilizzando un modello preconfigurato (Amazon Machine Image o AMI). All'avvio di un' EC2 istanza, installa EC2 automaticamente il sistema operativo (Linux o Microsoft Windows) e il software aggiuntivo incluso nell'AMI, come il software del server Web o del database.

Se ospiti un sito Web o esegui un'applicazione Web su un' EC2 istanza, puoi indirizzare il traffico dal tuo dominio, ad esempio example.com, al tuo server utilizzando Route 53. Per ulteriori informazioni, consulta Instradamento del traffico verso un'istanza Amazon EC2 .

AWS Elastic Beanstalk

Se utilizzi AWS Elastic Beanstalk per distribuire e gestire applicazioni nel AWS Cloud, puoi utilizzare Route 53 per indirizzare il traffico DNS per il tuo dominio, ad esempio example.com, verso un ambiente Elastic Beanstalk. Per ulteriori informazioni, consulta Instradamento del traffico verso un ambiente AWS Elastic Beanstalk.

Sistema di bilanciamento del carico elastico

Se ospiti un sito Web su più EC2 istanze Amazon, puoi distribuire il traffico verso il tuo sito Web tra le istanze utilizzando un sistema di bilanciamento del carico Elastic Load Balancing (ELB). Il servizio ELB ridimensiona automaticamente il load balancer al variare del traffico verso il tuo sito Web nel corso del tempo. Il load balancer, inoltre, è in grado di monitorare lo stato delle istanze registrate e instradare il traffico di dominio solo alle istanze integre.

Puoi utilizzare Route 53 per instradare il traffico per il tuo dominio al Classic, Application o Network Load Balancer. Per ulteriori informazioni, consulta Routing del traffico a un load balancer ELB.

Amazon Lightsail

Amazon Lightsail fornisce capacità di calcolo, archiviazione e rete e funzionalità per distribuire e gestire siti Web, applicazioni Web e database nel cloud a un prezzo mensile contenuto e prevedibile.

Se usi Lightsail, puoi usare Route 53 per instradare il traffico alla tua istanza Lightsail. Per ulteriori informazioni, consulta Utilizzo di Route 53 per puntare un dominio a un'istanza Amazon Lightsail.

Amazon S3

Amazon Simple Storage Service (Amazon S3) fornisce un'archiviazione nel cloud sicura, durevole e altamente scalabile. È possibile configurare un bucket S3 per ospitare siti Web statici che possono includere pagine Web e script lato client. (S3 non supporta lo scripting lato server). Puoi utilizzare Route 53 per instradare il traffico a un bucket Amazon S3. Per ulteriori informazioni, consulta i seguenti argomenti:

- Per ulteriori informazioni sul routing del traffico a un bucket, consulta Routing del traffico a un sito Web ospitato in un bucket Amazon S3.
- Per ulteriori informazioni sull'hosting di un sito Web statico in un bucket S3, consulta Nozioni di base su Amazon Route 53.

Amazon Virtual Private Cloud (Amazon VPC) (Amazon VPC)

Un endpoint di interfaccia ti consente di connetterti a servizi alimentati da. AWS PrivateLink Questi servizi includono alcuni AWS servizi, servizi ospitati da altri AWS clienti e partner propri VPCs (denominati servizi endpoint) e servizi Marketplace AWS partner supportati.

Puoi utilizzare Route 53 per instradare il traffico a un endpoint di interfaccia. Per ulteriori informazioni, consulta Routing del traffico a un endpoint di interfaccia di Amazon Virtual Private Cloud usando il proprio nome dominio.

Amazon WorkMail

Se utilizzi Amazon WorkMail per la tua e-mail aziendale e utilizzi Route 53 come servizio DNS, puoi utilizzare Route 53 per indirizzare il traffico verso il tuo dominio di WorkMail posta elettronica Amazon. Per ulteriori informazioni, consulta Instradamento del traffico verso Amazon WorkMail.

Per ulteriori informazioni, consulta . Instradamento del traffico Internet verso le tue risorse AWS.

Formato del nome dominio DNS

I nomi dominio (inclusi i nomi dei domini, zone ospitate e registri) sono costituiti da una serie di etichette separate da punti. Ogni etichetta può avere fino a 63 byte. La lunghezza totale di un nome dominio non può superare i 255 byte, inclusi i punti. Amazon Route 53 supporta qualsiasi nome dominio valido.

I requisiti di denominazione dipendono dal fatto che stai registrando un nome dominio o stai specificando il nome di una zona ospitata o un registro. Vedi l'argomento relativo.

Argomenti

Formattazione dei nomi dominio per la registrazione del nome dominio

Per la registrazione del nome dominio, un nome dominio può contenere solo i caratteri a-z, 0-9 e - (trattino). Non puoi specificare un trattino all'inizio o alla fine di un'etichetta.

Per ulteriori informazioni su come registrare un nome dominio internazionalizzato (IDN), consulta Formattazione di nomi dominio internazionalizzati.

Formattazione dei nomi dominio per zone ospitate e registri

Per zone ospitate e registri, il nome dominio può includere i seguenti caratteri ASCII stampabili (esclusi gli spazi):

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

Amazon Route 53 archivia i caratteri alfabetici come lettere minuscole (a-z), indipendentemente dal modo in cui li specifichi: come lettere maiuscole, minuscole o lettere corrispondenti in codici di escape.

Se il tuo nome di dominio contiene uno dei seguenti caratteri, devi specificare i caratteri utilizzando i codici di escape nel formato*three-digit octal code*:

- Caratteri da 000 a 040 ottali (da 0 a 32 decimali, da 0x00 a 0x20 esadecimali)
- Caratteri da 177 a 377 ottali (da 127 a 255 decimali, da 0x7F a 0xFF esadecimali)
- . (punto fermo), carattere 056 ottale (46 decimale, 0x2E esadecimale), quando utilizzato come carattere in un nome dominio. Quando usi . come delimitatore tra etichette, non devi utilizzare un codice di escape.

Se il nome di dominio include tutti i caratteri a a z, da 0 a 9, - (trattino) o _ (trattino basso), le operazioni API di Route 53 restituiscono i caratteri come codici di escape. Ciò è valido se devi specificare i caratteri come caratteri o come codici di escape quando si crea l'entità. La console Route 53 mostra i caratteri come caratteri, non come codici di escape.

Per un elenco dei caratteri ASCII e corrispondenti codici ottali, cerca su internet "tabella ascii".

Per specificare un nome dominio internazionalizzato (IDN), converti il nome in Punycode. Per ulteriori informazioni, consulta Formattazione di nomi dominio internazionalizzati.

Utilizza un asterisco (*) nei nomi di zone ospitate e registri

Puoi creare zone ospitate e registri che comprendano * nel nome.

Zona ospitata

- Non puoi includere un * nell'etichetta più a sinistra in un nome dominio. Ad esempio, *.esempio.com non è consentito.
- Se includi * in altre posizioni, il DNS lo considera un carattere * (ASCII 42), non come un carattere jolly.

Registri

Il DNS considera il carattere * sia come un carattere jolly che come il carattere * (ASCII 42), a seconda della posizione nel nome. Nota le seguenti limitazioni sull'utilizzo di * come carattere jolly nel nome di un registro:

- L'* deve sostituire l'etichetta più a sinistra in un nome dominio, ad esempio *.esempio.com o *.acme.esempio.com. Se includi * in qualsiasi altra posizione, come prod.*.esempio.com, il DNS lo considera un carattere * (ASCII 42), non un carattere jolly.
- L'* deve sostituire l'intera etichetta. Ad esempio, non puoi specificare *prod.esempio.com o prod*.esempio.com.
- I nomi dominio specifici hanno la precedenza. Ad esempio, se crei un registro per *.esempio.com e acme.esempio.com, Route 53 risponde sempre alle query DNS per acme.esempio.com con i valori nel registro acme.esempio.com.
- L'* si applica alle query DNS per il livello di sottodominio che include l'asterisco e a tutti i sottodomini di quel sottodominio. Ad esempio, se crei un registro denominato *.esempio.com, il Route 53 usa i valori in quel registro per rispondere alle query DNS per zenith.esempio.com, acme.zenith.esempio.com e pinnacle.acme.zenith.esempio.com (se non sono presenti registri per quella zona ospitata).

  Se crei un registro denominato *.esempio.com e non è presente un registro esempio.com, Route 53 risponderà alle query DNS per esempio.com con `NXDOMAIN` (dominio non esistente).
- Puoi configurare Route 53 per restituire la stessa risposta alle query DNS sia per tutti i sottodomini allo stesso livello sia per il nome dominio. Ad esempio, puoi configurare Route 53 per rispondere alle query DNS come acme.esempio.com e zenith.esempio.com utilizzando il registro esempio.com. Esegui queste fasi:

  1. Crea un registro per il dominio, ad esempio esempio.com.
  2. Crea un registro alias per il sottodominio, ad esempio *.esempio.com. Specifica il registro creato nella fase 1 come destinazione per il registro alias.
- Non puoi utilizzare * come carattere jolly per registri che presentano un tipo di NS.

Formattazione di nomi dominio internazionalizzati

Quando si registra un nuovo nome dominio o si creano zone ospitate e registri, è possibile specificare lettere diverse da a-z (ad esempio, la ç francese), caratteri in altri alfabeti (per esempio, cirillico o arabo) e caratteri in cinese, giapponese o coreano. Amazon Route 53 memorizza questi nomi di

dominio internazionalizzati (IDNs) in Punycode, che rappresenta i caratteri Unicode come stringhe ASCII.

Se stai registrando un nome dominio, tieni presente quanto segue:

- Puoi usare caratteri diversi da a-z, 0-9 e - (trattino) solo se il dominio di primo livello (TLD) supporta e supporta la lingua che desideri utilizzare. IDNs Per determinare quali lingue supporta il TLD, consulta Domini che è possibile registrare con Amazon Route 53.
- Puoi specificare un nome in una lingua non supportata se il nome contiene solo le lettere a-z. Ad esempio, se un TLD non supporta il francese ma il nome che desideri utilizzare include solo i caratteri a-z senza segni diacritici, puoi comunque utilizzarlo. In questo esempio, è consentito un nome che include una “c”; non lo è un nome che contiene una "ç".
- Se un TLD non supporta IDNs o non supporta la lingua che desideri utilizzare per il tuo nome di dominio, non puoi nemmeno specificare il nome in Punycode anche se il Punycode include solo a-z, 0-9 e -.

L'esempio seguente mostra la rappresentazione Punycode del nome dominio internazionalizzato 中国.asia:

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

Quando inserisci un IDN nella barra degli indirizzi di un browser moderno, il browser lo converte in Punycode prima di inviare una query DNS o creare una richiesta HTTP.

Il modo in cui si inserisce un IDN dipende da cosa si sta creando (nomi dominio, zone ospitate o registri) e dal modo in cui si crea (API, SDK o console Route 53):

- Se utilizzi l'API Route 53 o una di queste, puoi convertire a livello di codice un valore AWS SDKs Unicode in Punycode. Ad esempio, se stai utilizzando Java, puoi convertire un valore Unicode in Punycode utilizzando il metodo toASCII della libreria java.net.IDN.
- Se stai utilizzando la console Route 53 per registrare un nome dominio, è possibile incollare il nome, tra cui caratteri Unicode, nel campo del nome e la console converte il valore in Punycode prima di salvarlo.
- Se stai utilizzando la console Route 53 per creare zone ospitate o registri, devi convertire il nome dominio in Punycode prima di inserire il nome nel campo Nome applicabile. Per informazioni sui convertitori online, cerca su internet "convertitore punycode".

Se stai registrando un nome di dominio, tieni presente che non tutti i domini di primo livello () lo supportano. TLDs IDNs Per un elenco di quelli TLDs supportati da Route 53, vedi. Domini che è possibile registrare con Amazon Route 53 TLDs quelli che non supportano IDNs sono indicati.

Come registrare e gestire domini tramite Amazon Route 53

Se desideri ottenere un nuovo nome di dominio, ad esempio la parte esempio.com dell'URL http://esempio.com, puoi registrarlo con Amazon Route 53. Puoi anche trasferire la registrazione dei domini esistenti da altri registrar a Route 53 o trasferire la registrazione dei domini registrati con Route 53 a un altro registrar.

Le procedure in questo capitolo illustrano come registrarsi e trasferire domini utilizzando la console Route 53 e come modificare le impostazioni del dominio e visualizzare lo stato del dominio. Se stai registrando e gestendo solo pochi domini, usare la console è il modo più semplice.

Se hai bisogno di registrare e gestire un gran numero di domini, può essere più opportuno apportare modifiche a livello programmatico. Per ulteriori informazioni, consulta Configura Amazon Route 53.

> **Note**
>
> Se utilizzi un linguaggio per il quale esiste un AWS SDK, utilizza l'SDK anziché cercare di utilizzare il. APIs Semplificano l'autenticazione, si integrano facilmente con il tuo ambiente di sviluppo e forniscono un facile accesso ai comandi di Route 53. SDKs

I servizi di registrazione dei nomi a dominio sono forniti ai sensi del nostro Contratto per la registrazione del nome di dominio.

Argomenti

- Eliminazione della registrazione di un nome di dominio
- Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio
- Download di un report di fatturazione domini
- Domini che è possibile registrare con Amazon Route 53

Registrazione di nuovi domini

Questa sezione tratta i seguenti argomenti relativi alla registrazione di nuovi domini con Amazon Route 53:

1. Registrazione di un nuovo dominio:
   - Scopri la step-by-step procedura per registrare un nuovo dominio utilizzando la console Route 53.
   - Comprendi le considerazioni e i prerequisiti per la registrazione del dominio, come contattare l' AWS assistenza per problemi, prezzi, domini di primo livello supportati (TLDs) e creazione automatica di zone ospitate.
2. Valori specificati durante la registrazione o il trasferimento di un dominio:
   - Scopri i valori che devi fornire durante la registrazione o il trasferimento di un dominio, tra cui le informazioni di contatto, le impostazioni di protezione della privacy e le opzioni di rinnovo automatico.
   - Comprendi le implicazioni della modifica di determinati valori, come l'indirizzo email del proprietario del dominio o del registrante.
3. Valori restituiti da Amazon Route 53 durante la registrazione di un dominio:
   - Scopri i valori che Route 53 restituisce dopo una corretta registrazione del dominio, tra cui la data di registrazione, la data di scadenza, i codici di stato del dominio, lo stato del blocco del trasferimento e i name server.
4. Visualizzazione dello stato di una registrazione di dominio:
   - Scopri come visualizzare lo stato attuale della registrazione del tuo dominio, inclusi i codici di stato ICANN e tutte le azioni necessarie da parte tua, come la verifica dell'indirizzo email del registrante.

Registrazione di un nuovo dominio

Come registrare un nuovo dominio o aggiornare i name server di un dominio esistente

È possibile utilizzare Amazon Route 53 con i domini che record con Route 53, e con i domini registrati con altri provider DNS. A seconda del provider DNS, scegli una delle seguenti procedure per registrare e utilizzare un nuovo dominio con Route 53:

- Per registrare un nuovo dominio, consulta Come registrare un nuovo dominio utilizzando Route 53.
- Per un dominio esistente, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.
- Per spostare un dominio in un altro registrar, consulta come aggiornare i name server quando vuoi utilizzare un altro servizio DNS.

Considerazioni sulla registrazione del dominio

Prima di iniziare, tieni presente i seguenti punti:

Contattare l' AWS assistenza

Se riscontri problemi durante la registrazione di un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Prezzi di registrazione del dominio

Per informazioni sul costo per registrare domini, consulta Prezzi di Amazon Route 53 per la registrazione di domini.

Domini supportati

Per un elenco di quelli supportati TLDs, consultaDomini che è possibile registrare con Amazon Route 53.

Non è possibile modificare un nome di dominio dopo la registrazione

Se per errore viene registrato il nome di dominio errato, non è più possibile modificarlo. È necessario pertanto registrare un altro nome di dominio e specificare il nome corretto. Inoltre, non è possibile ottenere un rimborso per un nome di dominio registrato per errore.

AWS crediti

Non puoi utilizzare AWS i crediti per pagare la tariffa per la registrazione di un nuovo dominio con Route 53.

Prezzi speciali o premium

I record TLD hanno assegnato prezzi speciali o premium ad alcuni nomi di dominio. Non è possibile utilizzare Route 53 per registrare un dominio che ha un prezzo speciale o premium.

Costi per le zone ospitate

Quando record un dominio con Route 53, creiamo automaticamente una zona ospitata per il dominio e addebitiamo un piccolo canone mensile per la zona ospitata zone, oltre al costo annuale per la registrazione del dominio. Questa zona ospitata è il luogo in cui memorizzi informazioni su come indirizzare il traffico per il tuo dominio, ad esempio, verso un' EC2 istanza o una CloudFront distribuzione Amazon. Se non desideri utilizzare il dominio in questo momento, puoi eliminare la zona ospitata; se viene eliminata entro 12 ore dalla registrazione del dominio, non si verrà applicato alcun costo per la zona ospitata nella tua fattura AWS . Inoltre addebitiamo una piccola tariffa per le query DNS che riceviamo per il tuo dominio. Per ulteriori informazioni, consulta la pagina dei Prezzi Amazon Route 53.

Sostituzione della zona ospitata per un dominio

Se crei una nuova zona ospitata per un dominio, affinché il dominio utilizzi gli stessi name server della nuova zona ospitata devi aggiornare anche questi ultimi. Per informazioni dettagliate, consulta Sostituzione della zona ospitata per un dominio registrato con Route 53

Come registrare un nuovo dominio utilizzando Route 53

Come registrare un nuovo dominio utilizzando Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, seleziona Domini, quindi Domini registrati.
3. Nella pagina Domini registrati seleziona Registra domini.

    a. Nella sezione Cerca dominio inserisci il nome di dominio per cui desideri effettuare la registrazione e seleziona Cerca per scoprire se il nome di dominio è disponibile.

    Se il nome di dominio che vuoi registrare contiene caratteri diversi da a-z, A-Z, 0-9 e - (trattino), tieni presente quanto segue:

    - È possibile immettere il nome utilizzando i caratteri applicabili. Non è necessario convertire il nome in Punycode.

- Viene visualizzato un elenco di lingue. Scegli la lingua del nome specificato. Ad esempio, se immetti příklad ("esempio" in ceco), scegliere ceco (CES) o ceco (CZE).

  > **Note**
  >
  > Per le lingue con più di un codice, potrebbe essere necessario provarli entrambi. Anche se CES e CZE sono sinonimi, alcuni record TLD supportano solo uno dei due codici.

  Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

Se è disponibile, verrà visualizzato il dominio che hai inserito, altrimenti, verranno visualizzati come suggerimenti dei domini simili.

Puoi scegliere fino a cinque domini da registrare. I domini selezionati sono mostrati nell'elenco Domini selezionati.

b. Per eseguire la registrazione di più domini, ripeti i passaggi da 3a a 3b.

4. Seleziona Procedi all'acquisto.
5. Nella pagina Tariffe, scegli il numero di anni per cui desideri registrare il dominio e se vuoi che la registrazione del dominio sia rinnovata automaticamente prima della data di scadenza.

   > **Note**
   >
   > Le registrazioni dei nomi di dominio e i rinnovi non sono rimborsabili. Se si abilita il rinnovo automatico del dominio e si decide che non si vuole il nome del dominio dopo il rinnovo della registrazione, non è possibile ottenere un rimborso per il costo del rinnovo.

   Scegli Next (Successivo).
6. Nella pagina Informazioni di contatto, inserisci le informazioni di contatto del registrante del dominio, dell'amministratore, del tecnico e dei contatti di fatturazione. I valori inseriti in questa pagina vengono applicati a tutti i domini che stai registrando. Per ulteriori informazioni, consulta Valori specificati durante la registrazione o il trasferimento di un dominio.

> **Important**
>
> Il contatto che elenchi come registrante durante la registrazione del dominio avrà determinati diritti in qualità di titolare del nome di dominio registrato, ai sensi della Politica di trasferimento di ICANN. La maggior parte dei domini verrà eliminata alla chiusura dell'account Account AWS (per ulteriori informazioni, consultaIl mio AWS account è chiuso o definitivamente e il mio dominio è registrato con Route 53), tuttavia, se un dominio rimane in un account chiuso, il contatto che hai indicato come registrante potrebbe avere la possibilità di richiedere il trasferimento del nome di dominio a un registrar esterno. Pertanto, è importante che il contatto del registrante che elenchi sia tu o un'altra persona di cui ti fidi affinché agisca in modo responsabile.

Tieni presente le considerazioni seguenti:

Nome e cognome

Per First Name (Nome) e Last Name (Cognome), consigliamo di specificare il nome indicato nel tuo documento di identità ufficiale. Per alcune modifiche alle impostazioni di dominio, alcuni record di dominio richiedono di fornire una prova di identità. Il nome sul tuo ID deve corrispondere al nome del registrant per il dominio.

Contatti diversi

Per impostazione predefinita, utilizziamo le stesse informazioni per tutte e tre i contatti. Se desideri inserire informazioni diverse per uno o più contatti, imposta su off il toggle Uguale al registrant.

> **Note**
>
> Per i domini .it, il registrant e i contatti amministrativi devono corrispondere.

> **Note**
>
> Per i domini.jp, i contatti tecnici e amministrativi devono essere gli stessi.

Più domini

Se record più di un dominio, utilizziamo le stesse informazioni di contatto per tutti i domini.

Informazioni obbligatorie aggiuntive

Per alcuni domini di primo livello (TLDs), siamo tenuti a raccogliere informazioni aggiuntive. Per questi TLDs, inserisci i valori applicabili dopo il campo Codice postale/CAP.

Protezione della privacy

Scegli se desideri nascondere le informazioni di contatto dalle query WHOIS.

> **Note**
>
> È necessario specificare la stessa impostazione sulla privacy per i contatti amministrativi, di registrazione, tecnici e di fatturazione.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio
- Domini che è possibile registrare con Amazon Route 53

> **Note**
>
> Per attivare la protezione della privacy per i domini .uk, .me.uk e .org.uk, è necessario aprire una pratica di supporto e richiedere la protezione della privacy.

Scegli Next (Successivo).

7. Nella pagina Rivedi, esamina le informazioni inserite e, se lo desideri, correggile, leggi i termini di servizio e seleziona la casella di controllo per confermare di aver letto i termini del servizio.

   Scegli Invia.

8. Nel pannello di navigazione, seleziona Domini, quindi Richieste.

In questa pagina puoi visualizzare lo stato del dominio e anche se è necessario rispondere all'e-mail di verifica del contatto del registrant. Puoi anche decidere di inviare nuovamente l'e-mail di verifica.

Se per il contatto del registrant hai specificato un indirizzo e-mail che non è mai stato utilizzato per registrare un dominio con Route 53, alcuni registri TLD richiedono di verificare che l'indirizzo sia valido.

Inviamo un'e-mail di verifica da uno dei seguenti indirizzi e-mail:

- noreply@registrar.amazon — per la TLDs registrazione presso Amazon Registrar.
- noreply@domainnameverification.net — per la registrazione TLDs effettuata dal nostro registrar associato, Gandi. Per stabilire chi è il registrar per il tuo TLD, consulta Ricerca del registrar.

> **Important**
>
> Il registrant deve seguire le istruzioni nell'e-mail per verificare che l'e-mail è stata ricevuta oppure dobbiamo sospendere il dominio, secondo quanto stabilito da ICANN. Quando un dominio è sospeso, non è accessibile da Internet.

a. Quando ricevi l'e-mail di verifica, scegli il collegamento nell'e-mail che verifica se l'indirizzo e-mail è valido. Se non ricevi l'e-mail immediatamente, controlla la cartella di posta indesiderata.

b. Torna alla pagina Richieste. Se lo stato non si aggiorna automaticamente per comunicare che l'indirizzo e-mail è verificato, aggiorna il browser.

9. Quando la registrazione del dominio è completa, la fase successiva varia a seconda se desideri utilizzare Route 53 o un altro servizio DNS come servizio DNS per il dominio:

   - Route 53: nella hosted zone che Route 53 ha creato quando hai registrato il dominio, crea i record per indicare a Route 53 come desideri instradare il traffico per il dominio e i sottodomini.

     Ad esempio, quando un utente inserisce il tuo nome di dominio in un browser e la query viene inoltrata a Route 53, desideri che Route 53 risponda alla query con l'indirizzo IP di un server Web nel tuo data center o con il nome di un load balancer ELB?

Per ulteriori informazioni, consulta Utilizzo dei record.

> **Important**
>
> Se crei record in una zona ospitata diversa da quella creata automaticamente da Route 53, è necessario aggiornare i server di nomi affinché il dominio li utilizzi per la nuova zona ospitata.

- Un altro servizio DNS: configura il tuo nuovo dominio per instradare le query DNS all'altro servizio DNS. Esegui la procedura Come aggiornare i name server per utilizzare un altro registrar.

Valori specificati durante la registrazione o il trasferimento di un dominio

> **Note**
>
> Abbiamo aggiornato la console dei domini di Route 53. Durante il periodo di transizione, puoi utilizzare la nuova console o continuare a utilizzare la vecchia console. Le informazioni restituite da Route 53 sono per la maggior parte uguali per entrambe le console. Le differenze sono riportate nell'elenco seguente.

Quando record un dominio o ne trasferisci la registrazione ad Amazon Route 53, specifichi i valori che sono descritti in questo argomento.

> **Note**
>
> Se record più di un dominio, Route 53 usa i valori che hai specificato per tutti i domini che sono nel tuo carrello.

È possibile modificare i valori anche per un dominio che non è attualmente registrato con Route 53. Tieni presente quanto segue:

- Se modifichi le informazioni di contatto per il dominio, invieremo un'e-mail di notifica al registrant in merito alla modifica. Questa email proviene da noreply@registrar.amazon. Per la maggior parte delle modifiche, il registrant non è tenuto a rispondere.

- Per le modifiche alle informazioni di contatto che costituiscono anche una modifica di proprietà, inviamo al registrant un'ulteriore e-mail. ICANN richiede al registrant di confermare la ricezione dell'e-mail. Per ulteriori informazioni, consulta First Name, Last Name (Nome, Cognome) e Organization (Organizzazione) più avanti in questa sezione.

Per ulteriori informazioni sulla modifica delle impostazioni per un dominio esistente, consulta Come aggiornare le impostazioni di dominio .

Valori da specificare

- 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

Uguale al contatto del registrante

Specifica se si desidera utilizzare le stesse informazioni di contatto per il registrant del dominio, il contatto amministrativo e il contatto tecnico.

Tipo di contatto

Categoria per questo contatto. Tieni presente quanto segue:

- Se scegli un'opzione diversa da Person (Persona), è necessario inserire il nome di un'organizzazione.
- Per alcuni TLDs, la protezione della privacy disponibile dipende dal valore scelto per Tipo di contatto. Per le impostazioni di protezione della privacy per i tuoi TLD, consulta Domini che è possibile registrare con Amazon Route 53.
- Per i domini .es, il valore Contact Type (Tipo di contatto) deve essere Person (Persona) per tutti e tre i contatti.

Nome, cognome

Il nome e cognome del contatto.

> **Important**
>
> Per First Name (Nome) e Last Name (Cognome), consigliamo di specificare il nome indicato nel tuo documento di identità ufficiale. Per alcune modifiche alle impostazioni di dominio, è necessario fornire una prova di identità e il nome sul tuo ID deve corrispondere al nome del registrant del dominio.

Se stai trasferendo un dominio a Route 53 e le seguenti condizioni sono vere, stai modificando il proprietario del dominio:

- Il tipo di contatto è Person (Persona).
- Stai modificando i campi First Name (Nome) e/o Last Name (Cognome) per il contattato del registrant dalle impostazioni attuali.

In quel caso, ICANN richiede di inviare un'e-mail al registrant per ottenere l'approvazione. Inviamo un'e-mail da uno dei seguenti indirizzi e-mail:

TLDs	Indirizzo e-mail dal quale proviene l'approvazione
TLDs registrato da Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (L'e-mail viene inviata sia al vecchio registrant, sia al nuovo.)
Tutti gli altri	

TLDs	Indirizzo e-mail dal quale proviene l'approvazione
	noreply@domainnameverification.net

Per stabilire chi è il registrar per il tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

> **Important**
>
> Il registrant deve seguire le istruzioni nell'e-mail per confermare che l'e-mail è stata ricevuta oppure dobbiamo sospendere il dominio, secondo quanto stabilito da ICANN. Quando un dominio è sospeso, non è accessibile da Internet.

Se modifichi l'indirizzo e-mail di contatto per il registrant, quest'e-mail viene inviata al vecchio e al nuovo indirizzo e-mail di contatto per il registrant.

Alcuni registrar TLD addebitano una tariffa per la modifica del proprietario del dominio. Quando modifichi uno di questi valori, nella console Route 53 viene visualizzato un messaggio che indica se è previsto un costo.

Organizzazione

L'organizzazione che è associata al contatto, se del caso. Per il registrant e i contatti amministrativi, in genere è l'organizzazione che registra il dominio. Per il contatto tecnico, questa potrebbe essere l'organizzazione che gestisce il dominio.

Quando il tipo di contatto indica qualsiasi valore tranne Person (Persona) e si modifica il campo Organization (Organizzazione) per il registrant, è necessario modificare il proprietario del dominio. ICANN richiede di inviare un'e-mail al registrant per ottenere l'approvazione. Inviamo un'e-mail da uno dei seguenti indirizzi e-mail:

TLDs	Indirizzo e-mail dal quale proviene l'approvazione
TLDs registrato da Amazon Registrar	noreply@registrar.amazon
.fr	nic@nic.fr (L'e-mail viene inviata sia al vecchio registrant, sia al nuovo.)

TLDs	Indirizzo e-mail dal quale proviene l'approvazione
Tutti gli altri	noreply@domainnameverification.net

Per stabilire chi è il registrar per il tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

Se modifichi l'indirizzo e-mail di contatto per il registrant, quest'e-mail viene inviata al vecchio e al nuovo indirizzo e-mail di contatto per il registrant.

Alcuni registrar TLD addebitano una tariffa per la modifica del proprietario del dominio. Quando si modifica il valore di Organizzazione, nella console Route 53 viene visualizzato un messaggio che indica se è previsto un costo.

E-mail

L'indirizzo e-mail del contatto.

Se modifichi l'indirizzo e-mail di contatto per il registrant, inviamo un'e-mail di notifica al vecchio e al nuovo indirizzo e-mail di contatto per il registrant. Questa email proviene da noreply@registrar.amazon.

Telefono

Il numero di telefono del contatto:

- Se inserisci un numero di telefono per località negli Stati Uniti e in Canada, immetti 1 nel primo campo e l'indicativo di località a 10 cifre e il numero di telefono nel secondo campo.
- Se inserisci un numero di telefono per un'altra località, immetti il prefisso del paese nel primo campo e il resto del numero di telefono nel secondo. L'elenco dei prefissi telefonici internazionali è riportato alla pagina Wikipedia Prefissi telefonici internazionali.

Indirizzo 1

L'indirizzo del contatto.

Indirizzo 2

Ulteriori informazioni relative all'indirizzo del contatto, ad esempio il CAP o la casella postale.

Paese

Il paese del contatto.

Stato

La regione o la provincia del contatto.

Città

La città del contatto.

Codice di avviamento postale/CAP

Il codice di avviamento postale del contatto.

Campi per domini di primo livello selezionati

I seguenti domini di primo livello (TLDs) richiedono la specificazione di valori aggiuntivi:

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

Inoltre, molti TLDs richiedono un numero di identificazione IVA.

Per informazioni sui valori validi, ExtraParamconsulta Amazon Route 53 API Reference.

Protezione della privacy

Se desideri nascondere le informazioni di contatto dalle query WHOIS. Se selezioni Attiva protezione privacy (nuova console) o Nascondi informazioni di contatto (vecchia console), le query WHOIS (dall'inglese "who is", "chi è") restituiranno le informazioni di contatto relative al registrar o il valore "Protected by policy" (Protetto da policy).

> **Note**
>
> È necessario specificare la stessa impostazione di privacy per i contatti amministrativi, di registrazione, tecnici e di fatturazione.

Se selezioni Don't hide contact information (Non nascondere le informazioni di contatto), potrai ricevere più spam all'indirizzo e-mail specificato.

Chiunque può inviare una query WHOIS per un dominio e recuperare tutti i dati di contatto per quel dominio. Il comando WHOIS è disponibile in molti sistemi operativi, ed è disponibile anche come applicazione Web su molti siti web.

> **Important**
>
> Anche se ci sono utenti legittimi per le informazioni di contatto associate al tuo dominio, gli utenti più comuni sono gli spammer, che inviano ai contatti del dominio e-mail indesiderate e offerte false. In generale, ti consigliamo di selezionare Hide contact information (Nascondi informazioni di contatto) in Privacy Protection (Protezione della privacy).

Per attivare o disattivare la protezione della privacy per alcuni domini, è necessario aprire una pratica di supporto e richiedere la protezione della privacy.

Per ulteriori informazioni sulla protezione della privacy, consulta i seguenti argomenti:

- Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio
- Domini che è possibile registrare con Amazon Route 53

Rinnovo automatico (disponibile solo durante la modifica delle impostazioni di dominio)

Se si desidera che Route 53 rinnovi automaticamente il dominio prima della scadenza. La quota di registrazione viene addebitata sul tuo AWS account. Questa impostazione è disponibile sulla vecchia console solo quando si modificano le impostazioni del dominio. Per ulteriori informazioni, consulta Rinnovo della registrazione di un dominio.

> **Important**
>
> Se disattivi il rinnovo automatico, la registrazione per il dominio non verrà rinnovata alla data di scadenza e si potrebbe perdere il controllo del nome di dominio.

Il periodo durante il quale puoi rinnovare un nome di dominio varia a seconda del dominio di primo livello (TLD). Per una panoramica sul rinnovo dei domini, consulta Rinnovo della registrazione di

un dominio. Per informazioni su come estendere la registrazione del dominio per un determinato numero di anni, consulta Estendere il periodo di registrazione per un dominio.

Valori restituiti da Amazon Route 53 durante la registrazione di un dominio

Quando record il tuo dominio con Amazon Route 53, Route 53 restituisce i seguenti valori in aggiunta a quelli specificati.

Registrato il

La data in cui il dominio è stato originariamente registrato con Route 53.

Scade il

La data e l'ora in cui l'attuale periodo di registrazione scade, secondo fuso orario di Greenwich (GMT).

Il periodo di registrazione è in genere di un anno, sebbene i registri di alcuni domini di primo livello (TLDs) abbiano periodi di registrazione più lunghi. Per il periodo di registrazione e rinnovo del tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

Nella maggior parte dei casi TLDs, è possibile estendere il periodo di registrazione fino a dieci anni. Per ulteriori informazioni, consulta Estendere il periodo di registrazione per un dominio.

Codice di stato del nome di dominio

Lo stato corrente del dominio.

ICANN, l'organizzazione che gestisce un database centrale di nomi di dominio, ha sviluppato una serie di codici di stato dei nomi di dominio (noti anche come codici di stato EPP) che indicano lo stato di una serie di operazioni su un nome di dominio. Ad esempio, la registrazione di un nome di dominio, il trasferimento di un nome di dominio a un altro registrar, il rinnovo della registrazione per un nome di dominio e così via. Tutti i registrar utilizzano lo stesso set di codici di stato.

Per un elenco aggiornato dei codici di stato dei nomi di dominio e una spiegazione del significato di ciascun codice, visita il sito Web ICANN e cerca epp status codes (codici di stato EPP). (Consigliamo di eseguire la ricerca sul sito web dell'ICANN; talvolta le ricerche sul Web restituiscono una vecchia versione del documento).

Blocco del trasferimento

Se il dominio è bloccato per evitare che terzi possano trasferire il tuo dominio a un altro registrar senza la tua autorizzazione. Se il dominio è bloccato, il valore di Blocco trasferimento è impostato su On. Se il dominio non è bloccato, il valore è impostato su Off.

Rinnovo automatico

Se Route 53 rinnoverà automaticamente la registrazione per questo dominio poco prima della data di scadenza.

Codice di autorizzazione

Il codice necessario per trasferire la registrazione di questo dominio a un altro registrar. Un codice di autorizzazione viene generato solo quando viene richiesto. Per ulteriori informazioni sul trasferimento di un dominio a un altro registrar, consulta Trasferimento di un dominio da Amazon Route 53 a un altro registrar.

Server di nomi

I server Route 53 che rispondono alle query DNS per questo dominio. Si consiglia di non eliminare i server dei nomi Route 53.

Per ulteriori informazioni sull'aggiunta, modifica, eliminazione dei server di nomi, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

Visualizzazione dello stato di una registrazione di dominio

ICANN, l'organizzazione che gestisce un database centrale di nomi di dominio, ha sviluppato una serie di codici di stato dei nomi di dominio (noti anche come codici di stato EPP) che indicano lo stato di una serie di operazioni, ad esempio, la registrazione di un nome di dominio, il trasferimento di un nome di dominio a un altro registrar, il rinnovo della registrazione per un nome di dominio e così via. Tutti i registrar utilizzano lo stesso set di codici di stato.

Per visualizzare il codice di stato dei domini, esegui la seguente procedura.

Come visualizzare il codice di stato ICANN di un dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, espandi Domini, quindi seleziona Domini registrati.
3. Seleziona il nome collegato del dominio.

4. Se è necessario mettere in atto un'operazione, ad esempio inviare nuovamente l'e-mail di verifica al contatto del registrant, un banner nella parte superiore della pagina indicherà l'operazione da intraprendere.
5. Per lo stato attuale del tuo dominio, consulta il valore del campo Codice stato dominio.

   Per un elenco aggiornato dei codici di stato dei nomi di dominio e una spiegazione del significato di ciascun codice, visita il sito Web ICANN e cerca epp status codes (codici di stato EPP). (Consigliamo di eseguire la ricerca sul sito web dell'ICANN; talvolta le ricerche sul Web restituiscono una vecchia versione del documento).

Puoi visualizzare lo stato della registrazione anche nella pagina Richieste.

Come visualizzare lo stato della registrazione

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, espandi Domini, quindi seleziona Richieste.
3. Nella pagina Richieste, puoi visualizzare lo stato della registrazione e, inoltre, lo stato di qualsiasi altra operazione messa in atto sui domini, come l'eliminazione dei domini, il blocco dei trasferimenti di dominio, l'aggiunta o l'eliminazione di chiavi DNSSEC.

   Inoltre viene elencata ogni eventuale azione necessaria per completare un processo, come la verifica della tua e-mail.

   - Per rispondere a una richiesta di azione, seleziona il pulsante di opzione accanto al nome di dominio, quindi seleziona l'azione dal menu a discesa Azione.

Come aggiornare le impostazioni di dominio

Questa sezione fornisce informazioni sui seguenti argomenti relativi alla gestione delle impostazioni del dominio in Route 53:

1. Aggiornamento delle informazioni di contatto e di proprietà per un dominio:
   - Scopri come aggiornare le informazioni di contatto per un dominio, inclusi i contatti amministrativi, tecnici, del registrante e di fatturazione.
   - Comprendi la procedura per cambiare il proprietario di un dominio quando il registro richiede un modulo per il cambio di proprietà del dominio.

2. Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio:
   - Scopri come abilitare o disabilitare la protezione della privacy per le informazioni di contatto, che nasconde o rivela i tuoi dati personali dalle query WHOIS.
3. Abilitazione o disabilitazione del rinnovo automatico per un dominio:
   - Scopri come abilitare o disabilitare il rinnovo automatico di un dominio, che determina se Route 53 rinnova automaticamente la registrazione prima della scadenza.
4. Blocco di un dominio per evitare il trasferimento non autorizzato a un altro registrar:
   - Scopri come bloccare un dominio per impedire il trasferimento non autorizzato a un altro registrar e come disattivare il blocco quando necessario.
5. Estendere il periodo di registrazione per un dominio:
   - Comprendi la procedura per estendere il periodo di registrazione di un dominio, in genere fino a dieci anni con incrementi di un anno.
6. Come aggiornare i name server per utilizzare un altro registrareAggiunta o modifica di server di nomi e glue record per un dominio:
   - Scopri come aggiornare i name server per utilizzare un altro servizio DNS o configurare server di nomi white-label (vanity).
   - Scopri le considerazioni e le migliori pratiche per modificare i name server e incollare i record.

Aggiornamento delle informazioni di contatto e di proprietà per un dominio

Per i contatti amministrativi e tecnici per un dominio, è possibile modificare tutti i dati di contatto senza dover autorizzare le modifiche. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto per un dominio.

Per il registrant è possibile modificare la maggior parte dei valori senza dover autorizzare le modifiche. Tuttavia, per alcuni TLDs, la modifica del proprietario di un dominio richiede l'autorizzazione. Per ulteriori informazioni, consulta l'argomento applicabile.

Argomenti

- Chi è il proprietario di un dominio?
- TLDs che richiedono un'elaborazione speciale per cambiare il proprietario
- Aggiornamento delle informazioni di contatto per un dominio

- Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio

Chi è il proprietario di un dominio?

> **Important**
>
> Il contatto indicato come registrante avrà determinati diritti in quanto titolare del nome registrato del nome di dominio, ai sensi della Politica di trasferimento di ICANN. La maggior parte dei domini verrà eliminata alla chiusura del tuo account Account AWS (per maggiori informazioni, consultaIl mio AWS account è chiuso o definitivamente e il mio dominio è registrato con Route 53), tuttavia se un dominio rimane in un account chiuso, il contatto che hai indicato come registrante potrebbe avere la possibilità di richiedere il trasferimento del nome di dominio a un registrar esterno. Pertanto, è importante che il contatto del registrante che elenchi sia tu o un'altra persona di cui ti fidi affinché agisca in modo responsabile.

Quando il tipo di contatto è Person (Persona) e modifichi i campi First Name (Nome) o Last Name (Cognome) per il registrant, devi modificare il proprietario del dominio.

Quando il tipo di contatto è un valore qualsiasi eccetto Person (Persona) e modifichi Organization (Organizzazione), devi modificare il proprietario del dominio.

Notare quanto segue sulla modifica del proprietario di un dominio:

- Per alcuni TLDs, è prevista una commissione per cambiare il proprietario di un dominio. Per determinare se sono previsti costi per il TLD del dominio, consulta la colonna "Modifica del prezzo della proprietà" in Prezzi di Amazon Route 53 per la registrazione del dominio.

  > **Note**
  >
  > Non puoi utilizzare AWS i crediti per pagare l'eventuale commissione per cambiare il proprietario di un dominio.

- Per alcuni TLDs, quando cambi il proprietario di un dominio, inviamo un'email di autorizzazione all'indirizzo email di contatto del registrante. Il contatto del registrant deve seguire le istruzioni contenute nell'e-mail per autorizzare la modifica.

- Per alcuni TLDs, è necessario compilare un modulo per il cambio di proprietà del dominio e fornire un documento di identità in modo che un tecnico dell'assistenza di Amazon Route 53 possa aggiornare i valori per te. Se il TLD per il tuo dominio richiede un modulo di modifica di proprietà del dominio, la console visualizza un messaggio che consente di accedere a un modulo per aprire un caso di supporto. Per ulteriori informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

TLDs che richiedono un'elaborazione speciale per cambiare il proprietario

Quando si cambia il proprietario di un dominio, alcuni registri TLDs richiedono un'elaborazione speciale. Se stai modificando il proprietario per uno dei seguenti domini, esegui la procedura applicabile. Se si sta modificando il proprietario per qualsiasi altro dominio, è possibile eseguire l'operazione manualmente, a livello di codice o utilizzando la console Route 53. Per informazioni, consulta Aggiornamento delle informazioni di contatto per un dominio.

Quanto segue TLDs richiede un'elaborazione speciale per modificare il proprietario del dominio:

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

.be

È necessario ottenere un codice di trasferimento dal registro per i domini.be e quindi aprire un caso con Support AWS .

- Per ottenere il codice di trasferimento, consulta https://www.dnsbelgium. be/en/manage-your-domain-name/change-hold #transfer e segui le istruzioni.
- Per aprire un caso, vedi Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

.cl

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.com.ar

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.com.br

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.es

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.fi

Avvia la modifica del proprietario sulla console Route 53. Dopo aver avviato la modifica, riceverai una chiave di trasferimento Holder dall'indirizzo e-mail fi-domain-tech@traficom .fi. Dopo aver ricevuto la chiave, apri una richiesta di assistenza con AWS Support e condividi il codice della chiave con noi. Per informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

.qa

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.ru

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.se

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

.sh

È necessario compilare e inviare un modulo a AWS Support. Per informazioni, consulta Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio.

Aggiornamento delle informazioni di contatto per un dominio

Per aggiornare le informazioni di contatto per un dominio, eseguire la procedura seguente.

Come aggiornare le informazioni di contatto per un dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Seleziona il nome del dominio per cui desideri aggiornare le informazioni di contatto.
4. Nella scheda Informazioni di contatto seleziona Modifica.
5. Se non hai accesso all'indirizzo e-mail del contatto del registrante, procedi nel seguente modo. Se hai accesso all'indirizzo e-mail del contatto del registrante, vai al passaggio 6.

   a. Cambia solo l'indirizzo e-mail di contatto per il registrant. Non cambiare altri valori di uno dei contatti per il dominio. Per modificare anche altri valori, è possibile modificarli in un secondo momento nel processo.

      Scegli Save changes (Salva modifiche).

      Per verificare il nuovo indirizzo e-mail, inviamo un'e-mail di verifica al nuovo indirizzo (se richiesto per il TLD). È necessario scegliere il collegamento nell'e-mail per verificare che il nuovo indirizzo e-mail sia valido. Se è richiesta la verifica e non si verifica il nuovo indirizzo e-mail, Route 53 sospenderà il dominio come richiesto da ICANN.

      Se hai bisogno che l'e-mail di verifica sia nuovamente inviata, vai alla pagina Domini registrati, seleziona il pulsante di opzione accanto al nome di dominio che hai aggiornato e scegli il nome del dominio che intendi aggiornare. Nel messaggio di avviso Verifica la tua e-mail per evitare la sospensione del dominio, seleziona Invia e-mail nuovamente.

   b. Se desideri modificare altri valori per il registrante, l'amministratore, il tecnico o i contatti di fatturazione per il dominio, torna al passaggio 1 e ripeti la procedura.
6. Aggiorna i valori applicabili. Puoi anche selezionare Copia contatto registrant per inserire automaticamente le stesse informazioni inserite per il contatto del registrant. Per ulteriori informazioni, consulta Valori specificati durante la registrazione o il trasferimento di un dominio.

   A seconda del TLD per il tuo dominio e i valori che desideri modificare, la console potrebbe visualizzare il seguente messaggio:

"To change the registrant name or organization, open a case" (Per modificare il nome del registrant o l'organizzazione, aprire un caso).

Se il messaggio viene visualizzato, ignorare il resto della procedura e vedere Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio per ulteriori informazioni.

7. Seleziona Salva.
8. Se modifichi il proprietario del dominio, come illustrato in Chi è il proprietario di un dominio?, invieremo una e-mail al registrant per il dominio. L'indirizzo e-mail verrà richiesto per definire le autorizzazioni per la modifica del proprietario.

   Se non riceviamo l'autorizzazione per la modifica entro 3-15 giorni, a seconda del dominio di primo livello, dobbiamo annullare la richiesta, secondo quanto stabilito da ICANN.

   Le e-mail provengono da uno dei seguenti indirizzi e-mail.

TLDs	Indirizzo e-mail dal quale proviene l'autorizzazione
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
Tutti gli altri	Uno dei seguenti indirizzi e-mail: • noreply@registrar.amazon • noreply@domainnameverification.net

9. Se riscontri problemi durante l'aggiornamento delle informazioni di contatto, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Per informazioni sull'API che puoi utilizzare per aggiornare le informazioni di contatto, consulta UpdateDomainContact.

Modifica del proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio

Se il registro del dominio richiede il completamento di un cambio di proprietà del dominio e l'invio del modulo a AWS Support, esegui la procedura seguente. Per determinare se è necessario eseguire questa procedura, vedi i seguenti argomenti:

- Per determinare se il valore che si desidera modificare è considerata una modifica del proprietario, consulta Chi è il proprietario di un dominio?.
- Per determinare se è necessario un modulo di modifica di proprietà del dominio, consulta TLDs che richiedono un'elaborazione speciale per cambiare il proprietario.

Come modificare il proprietario di un dominio quando il record richiede un modulo di modifica di proprietà del dominio

1. Vedi l'introduzione a questo argomento per determinare se il record per il tuo dominio richiede l'elaborazione speciale per modificare il proprietario del dominio. In caso affermativo, e se un modulo Modifica di proprietà del dominio è obbligatorio, continuare con questa procedura.

   Se non è richiesto un modulo Modifica di proprietà del dominio, eseguire la procedura presente nell'argomento relativo.
2. Scarica il modulo di modifica di proprietà del dominio. Il file viene compresso in un file .zip.
3. Compila il modulo.
4. Per i contatti del registrant del precedente proprietario del dominio e del nuovo proprietario, ottenere copia di una prova di identità firmata (carta di identità, patente di guida, passaporto o altra prova legale di identità).

   Inoltre, se un'entità legale è elencata come organizzazione registrant, raccogliere le seguenti informazioni sul precedente proprietario del dominio e sul nuovo proprietario:

   - Prova dell'esistenza dell'organizzazione a cui il dominio è registrato.
   - Prova che i rappresentanti dell'ex proprietario e del nuovo proprietario sono autorizzati ad agire per conto dell'organizzazione. Questo documento deve essere un documento legale

certificato contenente sia il nome dell'organizzazione che il nome dei rappresentanti come firmatari (ad esempio, CEO e presidente, oppure Direttore esecutivo).

5. Eseguire la scansione del modulo di modifica di proprietà del dominio e della prova richiesta. Salva i documenti digitalizzati in un formato comune, ad esempio un file PDF o un file PNG.
6. Utilizzando l' AWS account su cui è attualmente registrato il dominio, accedi al AWS Support Center.

> **Important**
>
> Devi accedere utilizzando l'account root o tramite un utente a cui sono state concesse le autorizzazioni IAM in uno o più dei seguenti modi:
>
> - All'utente viene assegnata la policy AdministratorAccessgestita.
> - All'utente viene assegnata la policy DomainsFullAccess gestita AmazonRoute53.
> - All'utente viene assegnata la politica FullAccess gestita AmazonRoute53.
>
> Se non accedi utilizzando l'account root o un utente in possesso delle autorizzazioni necessarie, non saremo in grado di aggiornare il proprietario del dominio. Questo requisito impedisce agli utenti non autorizzati di modificare il proprietario di un dominio.

7. Specifica i seguenti valori:

   Regarding (Motivo)

   Accetta il valore predefinito di Account e fatturazione.

   Servizio

   Accetta il valore predefinito di Domains.

   Categoria

   Accetta il valore predefinito di Change of Ownership.

   Gravità

   Accetta il valore predefinito di Domanda generale.

   Scegli Next step: Additional information (Fase successiva: ulteriori informazioni)

Subject

Specifica Change the owner of a domain (Modifica il proprietario di un dominio)

Descrizione

Inserisci le informazioni che seguono:

- Dominio per il quale desideri modificare il proprietario
- ID account a 12 cifre dell' AWS account su cui è registrato il dominio

Aggiungere un allegato

Carica i documenti scansionati nel passaggio 5.

Contact method (Modalità di contatto)

Specificare un metodo di contatto e immettere i valori applicabili.

8. Scegli Invia.

Un tecnico del AWS Support esamina le informazioni fornite e aggiorna le impostazioni. Il tecnico potrà contattarti quando l'aggiornamento è terminato o contattarti per ulteriori informazioni.

Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio

Quando si registra un dominio con Amazon Route 53 o lo si trasferisce a Route 53, per impostazione predefinita viene abilitata la protezione della privacy per tutti i contatti per il dominio. Questo in genere nasconde la maggior parte dei tuoi dati di contatto da query WHOIS ("Who is") e consente di ridurre la quantità di spam che si riceve. Quando abiliti la protezione della privacy, le tue informazioni di contatto vengono sostituite con le informazioni di contatto del registrar o con la frase “REDACTED FOR PRIVACY” (Nascosto per questioni di privacy) o “On behalf of <domain name> owner” (Per conto del proprietario di <nome dominio>).

Se scegli di disabilitare la protezione della privacy, devi disabilitarla per tutti i contatti di un dominio. Se disabiliti la protezione della privacy, chiunque può inviare una richiesta WHOIS per il dominio e, per la maggior parte dei domini di primo livello (TLDs), potrebbe essere in grado di ottenere tutte le informazioni di contatto fornite al momento della registrazione o del trasferimento del dominio, inclusi nome, indirizzo, numero di telefono e indirizzo e-mail. Il comando WHOIS è ampiamente disponibile; è incluso in molti sistemi operativi, ed è disponibile anche come applicazione Web su molti siti web.

Se stai trasferendo un dominio a un altro registrar e la protezione della privacy è abilitata per i contatti del dominio, l'e-mail di verifica del trasferimento verrà inviata dagli indirizzi identity-protect.org per i contatti registrati con Amazon Registrar. TLDs Per stabilire chi è il registrar per il tuo TLD, consulta Ricerca del registrar.

Le informazioni che è possibile nascondere dalla query WHOIS dipendono da due fattori principali:

Il record per il dominio di primo livello

La maggior parte dei record TLD nasconde tutte le informazioni di contatto automaticamente, alcuni consentono di scegliere di nascondere tutte le informazioni di contatto, alcuni consentono di nascondere solo alcune informazioni e alcuni non consentono di nascondere le informazioni.

Quando la protezione della privacy è abilitata su un dominio, le tue informazioni di contatto vengono sostituite con le informazioni di contatto del servizio di privacy o con l'espressione “REDACTED FOR PRIVACY” (“Nascosto per questioni di privacy”). Il servizio di protezione della privacy applica funzionalità di prevenzione dello spam (rotazione e SPF/DKIM/spam analisi degli indirizzi) e, nella maggior parte dei casi, inoltrerà automaticamente le e-mail che superano questi filtri. Tuttavia, non è consigliabile inviare e-mail critiche a indirizzi e-mail con protezione dalla privacy poiché il meccanismo antispam potrebbe impedirne l'inoltro.

Inoltre, la scelta del meccanismo di protezione della privacy utilizzato per un dominio non è configurabile e viene selezionata automaticamente dal sistema. I dati di contatto per il nostro servizio di protezione della privacy non possono essere aggiornati manualmente.

> **Note**
>
> Per attivare o disattivare la protezione della privacy per alcuni domini, è necessario aprire una pratica di supporto e richiedere la protezione della privacy. Per ulteriori informazioni, consulta la sezione relativa in Domini che è possibile registrare con Amazon Route 53:
>
> - .co.uk (Regno Unito)
> - .me.uk (Regno Unito)
> - .org.uk (Regno Unito)
> - .link

Il registrar

Quando registri un dominio con Route 53 o lo trasferisci a Route 53, il registrar per il dominio è Amazon Registrar o il nostro registrar associato, Gandi. Amazon Registrar e Gandi nascondono informazioni diverse per impostazione predefinita:

- Amazon Registrar: per impostazione predefinita, tutti i tuoi dati di contatto sono nascosti. Tuttavia, le normative per il record del TLD hanno la precedenza.
- Gandi: per impostazione predefinita, tutti i dati di contatto sono nascosti eccetto il nome dell'organizzazione, se presente. Tuttavia, le normative per il record del TLD hanno la precedenza.

  Per le aree geografiche TLDs che non consentono la protezione della privacy, le tue informazioni personali verranno contrassegnate come «oscurate» nella pagina Whois Directory Search sul sito web di Gandi. Tuttavia, le tue informazioni personali potrebbero essere disponibili nel record del dominio o sui siti Web WHOIS di terze parti.

Per scoprire quali informazioni sono nascoste per il TLD per il tuo dominio, consulta Domini che è possibile registrare con Amazon Route 53.

Se si desidera attivare o disattivare la protezione della privacy per un dominio registrato con Route 53, completare la procedura seguente.

Per abilitare o disabilitare la protezione della privacy per le informazioni di contatto di un dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Sceglie il nome del dominio per cui desideri attivare o disattivare la protezione della privacy.
4. Nella sezione Informazioni di contatto seleziona Modifica.
5. Nella sezione Protezione privacy scegli se nascondere o meno le informazioni di contatto. Devi specificare la stessa impostazione di privacy per tutti e quattro i contatti: amministratore, registrante, tecnico e fatturazione.

> **Note**
>
> Se la protezione della privacy non è supportata per il tuo TLD, non viene visualizzata la sezione Protezione privacy.

6. Scegli Save changes (Salva modifiche).
7. Se riscontri problemi durante l'attivazione o la disabilitazione della protezione della privacy, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Abilitazione o disabilitazione del rinnovo automatico per un dominio

Se si desidera modificare se Amazon Route 53 rinnova automaticamente la registrazione per un dominio poco prima della data di scadenza, oppure si desidera visualizzare le impostazioni correnti per il rinnovo automatico, completare la procedura seguente.

Tieni presente che non puoi utilizzare AWS i crediti per pagare la tariffa per il rinnovo della registrazione di un dominio.

> **Note**
>
> Assicurati di disattivare il rinnovo automatico se intendi cancellare il tuo AWS account. Altrimenti, continuerai a ricevere avvisi di rinnovo da AWS. Il tuo dominio, tuttavia, non verrà rinnovato, a meno che non riattivi il tuo account.

Come abilitare o disabilitare il rinnovo automatico per un dominio

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Selezionare il nome del dominio che si desidera aggiornare.
4. Nella sezione Dettagli, nel menu a discesa Azioni seleziona Attiva il rinnovo automatico

   Al messaggio Attivare il rinnovo automatico per <domain name>? acconsenti di versare il canone annuo, quindi seleziona Attiva.

   > **Note**
   >
   > Il prezzo indicato si riferisce al periodo di registrazione attuale ed è suscettibile a modifiche. Per ulteriori informazioni, consulta Tariffe Amazon Route 53 per la registrazione di un dominio.

5. Per disattivare il rinnovo automatico, seleziona Disattiva il rinnovo automatico nel menu a discesa Azioni.
6. Se riscontri problemi durante l'attivazione o la disabilitazione del rinnovo automatico, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Blocco di un dominio per evitare il trasferimento non autorizzato a un altro registrar

I registri di dominio generici TLDs e per molti dati geografici TLDs consentono di bloccare un dominio per impedire a qualcuno di trasferirlo a un altro registrar senza la tua autorizzazione. Per determinare se il record per il tuo dominio consente di bloccare il dominio, consulta Domini che è possibile registrare con Amazon Route 53. Se il blocco è supportato e si desidera bloccare il dominio, eseguire la procedura seguente. Puoi anche utilizzare la procedura per disabilitare il blocco se desideri trasferire un dominio a un altro registrar.

Come bloccare un dominio per evitare il trasferimento non autorizzato a un altro registrar

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, selezionare Registered Domains (Domini registrati).
3. Selezionare il nome del dominio che si desidera aggiornare.
4. Nella sezione Dettagli, nel menu a discesa Azioni, scegli Attiva blocco trasferimento o Disattiva blocco trasferimento, in base alla tua intenzione di attivare o disattivare il blocco del trasferimento.

   Per esaminare lo stato di avanzamento della richiesta, puoi accedere alla pagina Richieste.
5. Se riscontri problemi durante il blocco di un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Nella ricerca WHOIS questo stato viene visualizzato come segue: `clientTransferProhibited`. Alcuni TLDs potrebbero avere anche questi stati:

- `clientUpdateProhibited`
- `clientDeleteProhibited`

Estendere il periodo di registrazione per un dominio

Quando si registra un dominio con Amazon Route 53 o se ne trasferisce la registrazione a Route 53, il dominio viene configurato in modo che il rinnovo sia automatico. Il periodo di rinnovo automatico è in genere di un anno, sebbene i registri di alcuni domini di primo livello (TLDs) abbiano periodi di rinnovo più lunghi.

Tieni presente quanto segue:

Periodo massimo di rinnovo

Tutti i codici generici TLDs e molti codici nazionali TLDs consentono di estendere la registrazione del dominio per periodi più lunghi, in genere fino a dieci anni con incrementi di un anno. Per determinare se puoi estendere il periodo di registrazione per il tuo dominio, consulta Domini che è possibile registrare con Amazon Route 53. Se sono consentiti periodi di registrazione più lunghi, esegui la procedura seguente.

Limitazioni relative al rinnovo o all'estensione della registrazione di un dominio

Alcuni record TLD hanno limitazioni su quando è possibile rinnovare o estendere la registrazione di un dominio, per esempio, gli ultimi due mesi prima della scadenza del dominio. Anche se il record consente di estendere il periodo di registrazione per un dominio, potrebbe non consentirlo all'attuale numero di giorni prima della scadenza del dominio.

AWS crediti

Non puoi utilizzare AWS i crediti per pagare la commissione per l'estensione del periodo di registrazione di un dominio.

Come estendere il periodo di registrazione per il dominio

1. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, selezionare Registered Domains (Domini registrati).
3. Seleziona il nome del dominio per cui desideri estendere il periodo di registrazione.
4. Nella sezione Dettagli, nel menu a discesa Azioni, seleziona Rinnova registrazione dominio.
5. Nella finestra di dialogo Rinnova registrazioni domini, nel menu a discesa Periodo di rinnovo, scegli il numero di anni a cui desideri estendere la registrazione.

L'elenco mostra tutte le opzioni correnti in base alla data di scadenza corrente e il periodo di registrazione massimo consentito dal record per questo dominio. La data di scadenza con un certo numero di anni è elencata al di sotto della durata.

6. Seleziona Rinnova registrazione dominio.

   Quando riceviamo conferma dal record che hai aggiornato la data di scadenza, ti invieremo un'e-mail per confermare che abbiamo modificato la data di scadenza.

7. Se riscontri problemi durante l'estensione del periodo di registrazione per un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Come aggiornare i name server per utilizzare un altro registrar

Se vuoi spostare la gestione DNS su un altro registrar, è necessario aggiornare i name server a cui puntare

Per aggiornare i server di nomi del dominio quando desideri utilizzare un altro servizio DNS

1. Utilizza il processo fornito dal tuo servizio DNS per ottenere i server di nomi per il dominio.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
4. Seleziona il nome del dominio che desideri configurare per usare un altro servizio DNS.
5. Nella sezione Dettagli, nel menu a discesa Azioni seleziona Modifica name server.
6. Elimina i name server esistenti, quindi aggiungi i nomi dei name server ai name server ottenuti dal servizio DNS nella fase 1.
7. Scegli Save changes (Salva modifiche).
8. (Facoltativo) Una volta registrato il tuo dominio, elimina la zona ospitata creata automaticamente da Route 53. In questo modo non ti verranno addebitati costi per una zona ospitata che non utilizzi.

   a. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate).
   b. Selezionare il pulsante di opzione per la zona ospitata che ha lo stesso nome del dominio.
   c. Scegliere Delete zona ospitata (Elimina zona ospitata)
   d. Seleziona Confirm (Conferma) per confermare che desideri eliminare la zona ospitata.

Aggiunta o modifica di server di nomi e glue record per un dominio

Quando registri un dominio con Route 53, viene creata automaticamente una zona ospitata per il dominio, vengono assegnati quattro server dei nomi alla zona ospitata e si aggiorna la registrazione del dominio in modo da utilizzare questi server. In genere non occorre modificare queste impostazioni a meno che non si preferisca utilizzare un altro servizio DNS o i server di nomi white label.

Il numero massimo di name server per dominio in Route 53 è pari a 6.

> **Warning**
>
> Se modifichi i server di nomi immettendo i valori errati, specifichi gli indirizzi IP sbagliato nei record associati o elimini uno o più server di nomi senza specificarne di nuovi, il tuo sito o applicazione potrebbe non essere disponibile su Internet per un massimo di due giorni

Argomenti

Considerazioni relative alla modifica di server dei nomi e glue record

Considera i seguenti problemi prima di modificare la configurazione.

Argomenti

Si desidera rendere Route 53 il servizio DNS per il dominio

Se al momento stai utilizzando un altro servizio DNS e si desidera rendere che Route 53 sia il servizio DNS per il dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente per le istruzioni dettagliate su come migrare il servizio DNS a Route 53.

> **Important**
>
> Se non rispetti rigorosamente il processo di migrazione, il dominio potrebbe diventare non disponibile su Internet per un massimo di due giorni.

Si desidera utilizzare un altro servizio DNS

Se si desidera utilizzare un servizio DNS diverso da Route 53 per il dominio, utilizzare la procedura seguente per modificare i server di nomi per la registrazione del dominio con quelli forniti dall'altro servizio DNS.

> **Note**
>
> Se si modificano i server di nomi e Route 53 restituisce il messaggio di errore riportato di seguito, il record del TLD non riconosce i server dei nomi specificati come validi:
> `"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."`
> I registri TLD in genere supportano i name server forniti dai servizi DNS pubblici ma non supportano server DNS privati, come i server DNS configurati su EC2 istanze Amazon, a meno che il registro non disponga di indirizzi IP per quei name server. Route 53 non supporta l'utilizzo di server dei nomi non riconosciuti dal record TLD. Se si verifica questo errore, è necessario modificare i server dei nomi per Route 53 o per un altro servizio DNS pubblico.

Si desidera utilizzare i server dei nomi white label

Se vuoi che i nomi dei server di nomi siano sottodomini del nome di dominio, puoi creare server di nomi white label. (I server di nomi white label sono detti anche server di nomi vanity o privati). Ad esempio puoi creare server di nomi da ns1.esempio.com a ns4.esempio.com per il dominio esempio.com. Per utilizzare server di nomi white label, utilizza la procedura seguente per specificare gli indirizzi IP dei server di nomi anziché i nomi. Questi indirizzi IP sono noti come record associati.

Per ulteriori informazioni sulla configurazione di server di nomi white label, consulta Configurazione dei server di nomi white label.

Si desidera modificare i server dei nomi per un dominio .it

IName i server per il tuo dominio IT devono superare un controllo DNS. Ti consigliamo di controllare i server dei nomi all'indirizzo https://dns-check.nic.it/ prima di inviare la richiesta di modifica. Il record continua a rispondere alle query DNS utilizzando i server di nomi precedenti alla modifica. Se i server di nomi precedenti non sono più disponibili, il dominio risulta indisponibile su Internet.

> **Important**
>
> Ogni volta che modifichi i server dei nomi per un dominio, assicurati che il DNS risponda alle query con i nuovi server di nomi prima di eliminare il precedente servizio DNS o di eliminare la zona ospitata Route 53 che utilizzava i server dei nomi precedenti.

Per informazioni su come ottenere assistenza AWS per correggere i nomi dei server dei nomi con il registro dei domini.it, consulta. Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio

Aggiunta o modifica di server dei nomi o glue record

Per aggiungere o modificare i server dei nomi o i glue record, esegui la procedura seguente.

> **Note**
>
> Per impostazione predefinita, i resolver DNS in genere memorizzano nella cache i nomi dei server dei nomi per due giorni. Di conseguenza, le modifiche possono richiedere due giorni per essere applicate. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Per aggiungere o modificare server dei nomi o glue record per un dominio

1. Rivedere Considerazioni relative alla modifica di server dei nomi e glue record e risolvere gli eventuali problemi applicabili.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

3. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
4. Seleziona il nome del dominio per cui desideri modificare le impostazioni.
5. Nella sezione Dettagli, nel menu a discesa Azioni seleziona Modifica name server.
6. Nella finestra di dialogo Modifica name server, è possibile:

   - Modificare il servizio DNS del dominio in uno dei seguenti modi:
     - Sostituire i server di nomi di un altro servizio DNS con i server di nomi di una zona ospitata di Route 53
     - Sostituire i server dei nomi di una zona ospitata Route 53 con i server dei nomi di un altro servizio DNS
     - Sostituire i server dei nomi di una zona ospitata di Route 53 con i server dei nomi di un'altra zona ospitata di Route 53.

     Per informazioni su come modificare il servizio DNS per un dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente. Per informazioni su come ottenere i server dei nomi per la zona ospitata di Route 53 che desideri utilizzare per il servizio DNS per il dominio, consulta Ottenere i server di nomi per una zona ospitata pubblica.
   - Aggiungi uno o più server di nomi.
   - Sostituire il nome di un server di nomi esistente.
   - Se si specificano server dei nomi white-label, aggiungere o modificare gli indirizzi IP nei glue record. Puoi inserire gli indirizzi in IPv4 o in IPv6 formato. Se un server di nomi dispone di più indirizzi IP, inserisci ogni indirizzo su una riga separata.

     Un server dei nomi white-label include il nome di dominio, ad esempio example.com, nel nome del server dei nomi, ad esempio ns1.example.com. Quando si specifica un server dei nomi white-label, Route 53 richiede di specificare uno o più indirizzi IP per il server dei nomi. L'indirizzo IP è noto come un glue record. Per ulteriori informazioni, consulta Configurazione dei server di nomi white label.
   - Eliminare un nome server. Scegliere l'icona x sul lato destro del campo per quel server di nomi.

> **Warning**
>
> Se modifichi i server di nomi immettendo i valori errati, specifichi gli indirizzi IP sbagliato nei record associati o elimini uno o più server di nomi senza specificarne di nuovi, il tuo

sito o applicazione potrebbe non essere disponibile su Internet per un massimo di due giorni

7. Scegli Aggiorna.
8. Se riscontri problemi durante l'aggiunta o la modifica dei name server o i record di colla, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Rinnovo della registrazione di un dominio

Quando si registra un dominio con Amazon Route 53 o se ne trasferisce la registrazione a Route 53, il dominio viene configurato in modo che il rinnovo sia automatico. Il periodo di rinnovo automatico è in genere di un anno, sebbene i registri di alcuni domini di primo livello (TLDs) abbiano periodi di rinnovo più lunghi. Per il periodo di registrazione e rinnovo del tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

Note

Non puoi utilizzare i AWS crediti per pagare la tariffa per il rinnovo della registrazione di un dominio.

Per la maggior parte dei domini di primo livello (TLDs), puoi modificare la data di scadenza di un dominio. Per ulteriori informazioni, consulta Estendere il periodo di registrazione per un dominio.

Important

Per disattivare il rinnovo automatico, devi essere a conoscenza dei seguenti effetti sul tuo dominio:

- Alcuni record TLD cancellano i domini anche prima della data di scadenza se non viene effettuato il rinnovo con adeguato anticipo. Ti consigliamo di lasciare abilitato il rinnovo automatico se desideri mantenere un determinato nome di dominio.
- Ti consigliamo inoltre di non programmare di registrare nuovamente un dominio dopo la sua scadenza. Alcuni registrar consentono ad altre di registrare domini immediatamente dopo la loro scadenza, pertanto potrebbe non essere possibile effettuare una nuova registrazione prima che il dominio venga preso da qualcun altro.

- Alcuni record applicano un costo elevato per il ripristino dei domini scaduti.
- Alla data di scadenza o in prossimità della data di scadenza, il dominio non è più disponibile in Internet.

Per determinare se il rinnovo automatico è abilitato per il tuo dominio, consulta Abilitazione o disabilitazione del rinnovo automatico per un dominio.

Se il rinnovo automatico è abilitato, accade quanto descritto di seguito:

45 giorni prima della scadenza

Inviamo un'e-mail al registrant che indica che il rinnovo automatico è attualmente abilitato e fornisce istruzioni su come disattivarlo. tieni aggiornato l'indirizzo e-mail del contatto del registrant in modo che possa ricevere e leggere questa e-mail.

35 o 30 giorni prima della scadenza

Per tutti i domini eccetto i domini .com.ar, .com.br e .jp, rinnoviamo la registrazione del dominio 35 giorni prima della data di scadenza in modo da avere il tempo di risolvere qualsiasi problema con il rinnovo prima della scadenza del nome di dominio.

I record per i domini .com.ar, .com.br e .jp richiedono il rinnovo dei domini non più di 30 giorni prima della scadenza. Riceverai un'e-mail di rinnovo da Gandi, il nostro registrar associato, 30 giorni prima della scadenza, che è lo stesso giorno in cui rinnoviamo il tuo dominio se hai il rinnovo automatico abilitato.

> **Note**
>
> Quando rinnoviamo il tuo dominio, ti invieremo un'e-mail per informarti che lo abbiamo rinnovato. Se il rinnovo non è andato a buon fine, ti invieremo un'e-mail per spiegarti il perché.

Se il rinnovo automatico è disabilitato, ecco cosa succede quando si avvicina la data di scadenza di un nome di dominio:

45 giorni prima della scadenza

Inviamo un'e-mail al registrant del dominio che indica che il rinnovo automatico è attualmente disabilitato e fornisce istruzioni su come attivarlo. tieni aggiornato l'indirizzo e-mail del contatto del registrant in modo che possa ricevere e leggere questa e-mail.

30 giorni o 7 giorni prima della scadenza

Se il rinnovo automatico è disabilitato per il dominio, l'ICANN, l'ente che regola le registrazioni dei domini, richiede al registrar di inviarti un'e-mail. Le e-mail provengono da uno dei seguenti indirizzi e-mail:

- noreply@registrar.amazon — Per i domini per i quali il registrar è Amazon Registrar.
- noreply@domainnameverification.net: per i domini per i quali il registrar è il nostro registrar associato, Gandi.

Per stabilire chi è il registrar per il tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

Se il rinnovo automatico viene attivato meno di 30 giorni prima della scadenza e il periodo di rinnovo non è passato, il dominio viene rinnovato entro 24 ore.

> **Important**
>
> Alcuni registri TLD prevedono restrizioni su quando è possibile rinnovare un dominio. Per i dettagli specifici del tuo dominio, consulta. Domini che è possibile registrare con Amazon Route 53 Inoltre, l'elaborazione di un rinnovo può richiedere fino a un giorno. Se ritardi troppo prima di abilitare il rinnovo automatico, il dominio potrebbe scadere prima che il rinnovo possa essere elaborato e si potrebbero perdere il dominio. Se la data di scadenza si avvicina, ti consigliamo di estendere manualmente la data di scadenza del dominio. Per ulteriori informazioni, consulta Estendere il periodo di registrazione per un dominio.

Per ulteriori informazioni sui periodi di rinnovo, vedi la sezione Scadenze per il rinnovo e il ripristino dei domini per il TLD in Domini che è possibile registrare con Amazon Route 53.

Dopo la data di scadenza

Il registrar conserva per un breve periodo di tempo dopo la scadenza la maggior parte dei domini, quindi è possibile rinnovare un dominio scaduto dopo la data di scadenza, ma se vuoi mantenere un dominio è vivamente consigliato mantenere attivato il rinnovo automatico. Per informazioni

sul tentativo di rinnovo di un dominio dopo la data di scadenza, consulta Ripristino di un dominio scaduto o eliminato.

Se il dominio scade ma è consentito il rinnovo tardivo, puoi rinnovare il dominio al prezzo standard di rinnovo. Per determinare se un dominio è ancora all'interno del periodo di rinnovo tardivo, esegui la procedura descritta nella sezione Estendere il periodo di registrazione per un dominio. Se il dominio è ancora elencato, è nel periodo di rinnovo tardivo.

Per ulteriori informazioni sui periodi di rinnovo, vedi la sezione Scadenze per il rinnovo e il ripristino dei domini per il TLD in Domini che è possibile registrare con Amazon Route 53.

Ripristino di un dominio scaduto o eliminato

Se non rinnovi un dominio prima della fine del periodo di rinnovo tardivo o se lo elimini accidentalmente, per alcuni registri per domini di primo livello (TLDs), puoi ripristinare il dominio prima che diventi disponibile per la registrazione da parte di altri.

Quando un dominio viene eliminato o supera la fine del periodo di rinnovo tardivo, non appare più nella console Amazon Route 53.

> **Important**
>
> Il prezzo per il ripristino di un dominio è generalmente più alto e a volte molto più alto del prezzo per la registrazione o il rinnovo di un dominio. Per il prezzo attuale di ripristino di un dominio, consulta la colonna Prezzo di ripristino in Tariffe di Amazon Route 53 per la registrazione di domini.

Non puoi utilizzare i AWS crediti per pagare la commissione per il ripristino di un dominio scaduto.

Per tentare di ripristinare una registrazione di dominio quando un dominio viene eliminato o la fine del periodo di rinnovo è scaduta

1. Determina se il record TLD del dominio supporta il ripristino dei domini e, in caso affermativo, il periodo durante il quale è consentito il ripristino.
   a. Passa a Domini che è possibile registrare con Amazon Route 53.
   b. Individua il TLD del dominio ed esamina i valori nella sezione Scadenze per il rinnovo e il ripristino dei domini.

> **Important**
>
> Inoltreremo le richieste di ripristino a Gandi, che le elabora durante l'orario lavorativo dal lunedì al venerdì. Gandi ha sede a Parigi, dove il fuso è UTC/GMT+1 ora. Di conseguenza, a seconda del momento in cui invii una richiesta, in rari casi può essere necessaria una settimana o più per elaborarla.

2. Il prezzo per il ripristino di un dominio è generalmente più alto e a volte molto più alto del prezzo per la registrazione o il rinnovo di un dominio. In Tariffe Amazon Route 53 per la registrazione dei domini, individua il TLD per il dominio (ad esempio .com) e verifica il prezzo nella colonna Prezzo di ripristino. Se si desidera ripristinare il dominio, annotare il prezzo che sarà necessario in un secondo momento.
3. Utilizzando l' AWS account su cui è stato registrato il dominio, accedi al AWS Support Center.
4. Specifica i seguenti valori:

   Regarding (Motivo)

   Accetta il valore predefinito di Account e fatturazione.

   Servizio

   Accetta il valore predefinito di Domains.

   Categoria

   Accetta il valore predefinito di Restoration.

   Gravità

   Accettate il valore predefinito di Domanda generale.

   Scegli Next step: Additional information (Fase successiva: ulteriori informazioni)

   Subject

   Digita Restore an expired domain (Ripristina un dominio scaduto) o Restore a deleted domain (Ripristina un dominio eliminato).

   Descrizione

   Inserisci le informazioni che seguono:

- Il dominio che desideri ripristinare
- L'ID dell'account a 12 cifre dell' AWS account su cui è stato registrato il dominio
- Conferma che accetti il prezzo per ripristinare il dominio. Utilizza il seguente testo:

  "Accetto il prezzo di $ ____ per ripristinare il mio dominio".

  Inserisci nello spazio vuoto il prezzo che hai individuato nel passaggio 2.

Contact method (Modalità di contatto)

Specificare un metodo di contatto e immettere i valori applicabili.

5. Scegli Invia.
6. Quando sapremo se siamo riusciti a ripristinare il tuo dominio, un rappresentante del AWS Supporto ti contatterà. Inoltre, se siamo stati in grado di ripristinare il tuo dominio, il dominio verrà visualizzato nella console. La data di scadenza dipende dal fatto che il dominio sia scaduto o che sia stato eliminato accidentalmente:

   Il dominio è scaduto

   La nuova data di scadenza è di solito uno o due anni (a seconda del TLD) dopo la vecchia data di scadenza.

   > **Note**
   >
   > La nuova data di scadenza non viene calcolata a partire dalla data di ripristino del dominio.

   Il dominio è stato eliminato accidentalmente

   La data di scadenza in genere non cambia.

Sostituzione della zona ospitata per un dominio registrato con Route 53

Se elimini la zona ospitata per un dominio, è necessario creare un'altra zona ospitata quando sei pronto a rendere il dominio disponibile su Internet. Esegui la seguente procedura.

Per sostituire la zona ospitata per un dominio

1. Crea una zona ospitata pubblica Per ulteriori informazioni, consulta Creazione di una zona ospitata pubblica.
2. Crea record nella zona ospitata. I record definiscono il modo in cui si desidera instradare il traffico per il dominio (esempio.com) e i sottodomini (acme.esempio.com, zenith.esempio.com). Per ulteriori informazioni, consulta Utilizzo dei record.
3. Aggiorna la configurazione del dominio in modo che utilizzi i server di nomi per la nuova zona ospitata Per ulteriori informazioni, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

   > **Important**
   >
   > Quando crei una zona ospitata, Route 53 assegna un set di quattro server dei nomi alla zona ospitata. Se cancelli una zona ospitata e ne crei una, Route 53 assegna una altra serie composta da quattro name server. Di solito, nessun server di nomi per la nuova zona ospitata corrisponde ad alcun server di nomi per la precedente zona ospitata. Se non aggiorni la configurazione del dominio in modo che utilizzi i server di nomi per la nuova zona ospitata, il dominio rimarrà non disponibile su Internet.

4. Se riscontri problemi durante la sostituzione della zona ospitata per un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Trasferimento dei domini

È possibile trasferire la registrazione del dominio da un altro registrar ad Amazon Route 53, da un account AWS a un altro o da Route 53 a un altro registrar. Il trasferimento di domini da un AWS account a un altro è gratuito.

Gli argomenti di questa sezione riguardano i seguenti argomenti relativi al trasferimento di domini:

1. Trasferimento della registrazione per un dominio ad Amazon Route 53
   - Scopri la step-by-step procedura per trasferire un dominio da un altro registrar a Route 53, inclusi i prerequisiti, i codici di autorizzazione e l'aggiornamento delle impostazioni DNS.
   - Scopri come il trasferimento di un dominio influisce sulla data di scadenza e sulle considerazioni relative ai diversi domini di primo livello (). TLDs

2. Visualizzazione dello stato di un trasferimento di dominio
   - Scopri come visualizzare lo stato di una richiesta di trasferimento di dominio e il significato dei diversi codici di stato durante il processo di trasferimento.
3. Come il trasferimento di un dominio ad Amazon Route 53 influenza la data di scadenza della registrazione del dominio
   - Scopri come il trasferimento di un dominio su Route 53 potrebbe influire sulla data di scadenza del dominio.
4. Trasferimento di un dominio su un altro account AWS
   - Scopri come trasferire un dominio da un AWS account a un altro, inclusi i ruoli e le autorizzazioni necessari per avviare e accettare il trasferimento.
   - Scopri il passaggio facoltativo di migrazione della zona ospitata al nuovo account dopo il trasferimento del dominio.
5. Trasferimento di un dominio da Amazon Route 53 a un altro registrar
   - Comprendi il processo di trasferimento di un dominio da Route 53 a un altro registrar, incluso l'ottenimento del codice di autorizzazione, l'aggiornamento delle impostazioni DNS e la risposta alle e-mail di conferma.
   - Tieni presente le considerazioni relative al trasferimento del servizio DNS a un altro provider e il potenziale impatto sulle funzionalità specifiche di Route 53, come i record di alias e le politiche di routing.

Seguendo le informazioni fornite negli argomenti sopra elencati, è possibile trasferire in modo efficace i domini da e verso Route 53, gestire il processo di trasferimento e garantire una transizione fluida mantenendo la configurazione e il routing DNS corretti.

Trasferimento della registrazione per un dominio ad Amazon Route 53

> **Important**
>
> Durante il trasferimento di qualsiasi dominio di primo livello nazionale (ccTLDs) su Route 53, ad eccezione di .cc e .tv, gli aggiornamenti al contatto del proprietario vengono ignorati e vengono utilizzati i dati di contatto del proprietario del registro. Una volta completato il trasferimento, puoi aggiornare le informazioni di contatto del proprietario. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto e di proprietà per un dominio.

Per trasferire la registrazione di un dominio ad Amazon Route 53, attieniti alle procedure descritte di seguito.

> **Important**
>
> Se salti una fase, il tuo dominio potrebbe non essere disponibile su Internet.

Tieni presente quanto segue:

Contattare l' AWS assistenza

Se riscontri problemi durante il trasferimento di un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Data di scadenza

Per informazioni su come il trasferimento del tuo dominio interessa l'attuale data di scadenza, consulta Come il trasferimento di un dominio ad Amazon Route 53 influenza la data di scadenza della registrazione del dominio.

Costo del trasferimento

Quando trasferisci un dominio su Route 53, la commissione di trasferimento che applichiamo al tuo AWS account dipende dal dominio di primo livello, ad esempio.com o.org. Per ulteriori informazioni, consultare Prezzi di Route 53.

Non puoi utilizzare AWS i crediti per pagare l'eventuale commissione per il trasferimento di un dominio su Route 53.

> **Note**
>
> Route 53 addebita la tariffa di trasferimento del dominio prima di avviare il processo di trasferimento. Se un trasferimento non va a buon fine per qualsiasi motivo, il costo del trasferimento viene accreditato immediatamente sul tuo account.

Nomi di dominio speciali e premium

I record TLD hanno assegnato prezzi speciali o premium ad alcuni nomi di dominio. Non è possibile trasferire un dominio a Route 53 se il dominio ha un prezzo speciale o premium.

Quote di domini

Il numero massimo predefinito di domini per AWS account è 20. È possibile richiedere una quota più elevata. Per ulteriori informazioni, consulta Quote relative ai domini.

Limite dei name server

Il numero massimo di name server per dominio in Route 53 è pari a 6.

Argomenti

Requisiti per il trasferimento dei domini di primo livello

La maggior parte dei registrar di domini applicano requisiti specifici sul trasferimento di un dominio a un altro registrar. Lo scopo principale di questi requisiti è impedire ai proprietari di domini fraudolenti di trasferire ripetutamente i domini a diversi registrar. I requisiti variano, ma i seguenti sono generalmente comuni:

- È necessario avere registrato il dominio con l'attuale registrar o aver trasferito la registrazione del dominio per il registrar corrente da almeno 60 giorni.
- Se la registrazione per un nome di dominio è scaduta ed è stato necessario ripristinarla, il ripristino deve essere stato effettuato almeno 60 giorni prima.
- Il dominio non può avere uno dei seguenti codici di stato del nome di dominio:
  - clientTransferProhibited
  - pendingDelete

- pendingTransfer
- redemptionPeriod
- serverTransferProhibited

- I record per alcuni domini di primo livello non consentono il trasferimento fino al termine delle modifiche, ad esempio quelle al proprietario del dominio.

Per un elenco aggiornato dei codici di stato dei nomi di dominio e una spiegazione del significato di ciascun codice, visita il sito Web per ICANN e cerca codici di stato EPP. (Consigliamo di eseguire la ricerca sul sito web dell'ICANN; talvolta le ricerche sul Web restituiscono una vecchia versione del documento).

> **Note**
>
> ICANN è l'organizzazione che stabilisce i criteri che disciplinano il trasferimento e la registrazione di nomi di dominio.

È inoltre possibile cercare il nome di dominio sul sito Web di Whois per visualizzare i codici di stato e altre informazioni relative al dominio.

Fase 1: Conferma che Amazon Route 53 supporti i domini di primo livello

Per informazioni, consulta Domini che è possibile registrare con Amazon Route 53. Se il dominio di primo livello per il dominio che si desidera trasferire è incluso nell'elenco, è possibile trasferire il dominio ad Amazon Route 53.

Se un TLD non è presente nell'elenco, non è possibile trasferire la registrazione di dominio a Route 53. Occasionalmente ne aggiungiamo altri TLDs all'elenco, quindi ricontrolla per vedere se abbiamo aggiunto il supporto per il tuo dominio.

Fase 2 (facoltativa): trasferisci il tuo servizio DNS ad Amazon Route 53 o a un altro provider di servizi DNS

Perché trasferire prima il servizio DNS?

Alcuni registrar forniscono un servizio DNS gratuito che potrebbe essere disabilitato non appena ricevono una richiesta dalla Route 53 per trasferire la registrazione del dominio. Se si desidera che

Route 53 fornisca il servizio DNS per il proprio dominio, consultare Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Fase 3: Modifica delle impostazioni con il registrar corrente

Utilizzando il metodo fornito dal registrar corrente, completare le attività riportate di seguito per ogni dominio che si desidera trasferire.

- 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)

Conferma che l'e-mail di contatto del registrant per il tuo dominio sia aggiornata

Invieremo una e-mail a tale indirizzo per richiedere l'autorizzazione al trasferimento. È necessario fare clic su un collegamento nell'e-mail per autorizzare il trasferimento. Se non fai clic sul link, annulleremo il trasferimento.

> **Important**
>
> Il contatto che elenchi come registrante avrà determinati diritti in qualità di titolare del nome registrato del nome di dominio, ai sensi della Politica di trasferimento di ICANN. La maggior parte dei domini verrà eliminata alla chiusura del tuo account Account AWS (per maggiori informazioni, consultaIl mio AWS account è chiuso o definitivamente e il mio dominio è registrato con Route 53), tuttavia se un dominio rimane in un account chiuso, il contatto che hai indicato come registrante potrebbe avere la possibilità di richiedere il trasferimento del nome di dominio a un registrar esterno. Pertanto, è importante che il contatto del registrante che elenchi sia tu o un'altra persona di cui ti fidi affinché agisca in modo responsabile.

Sblocca il dominio in modo che possa essere trasferito

ICANN, l'ente che regola le registrazioni dei domini, richiede di sbloccare il dominio prima di trasferirlo.

Conferma che lo stato del dominio consenta di trasferire il dominio

Per ulteriori informazioni, consulta Requisiti per il trasferimento dei domini di primo livello.

Disabilitazione di DNSSEC per il dominio

Se si utilizza DNSSEC con un dominio e si trasferisce la registrazione del dominio a Route 53, è necessario disabilitare il protocollo DNSSEC nel registrar precedente. Quindi, dopo aver trasferito la registrazione del dominio, eseguire le operazioni per impostare il DNSSEC per il dominio in Route 53. Route 53 supporta DNSSEC per la registrazione del dominio, ma non per la firma del DNSSEC. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

> **Important**
>
> Se si trasferisce una registrazione di dominio a Route 53 mentre il DNSSEC è configurato, vengono trasferite anche le chiavi pubbliche DNSSEC. Se si trasferisce il servizio DNS a un provider che non supporta DNSSEC, la risoluzione DNS non riesce in modo intermittente fino a quando non si eliminano le chiavi DNSSEC dal dominio. Per ulteriori informazioni, consulta Eliminazione di chiavi pubbliche per un dominio.

Ottieni un codice di autorizzazione

Un codice di autorizzazione fornito dall'attuale registrar ci autorizza a richiedere che la registrazione per il dominio venga trasferita a Route 53. Questo codice dovrà essere specificato nella console Route 53 in un secondo momento.

Alcuni domini di primo livello hanno requisiti aggiuntivi:

Domini .co.za

Non è necessario ottenere un codice di autorizzazione per trasferire un dominio .co.za a Route 53.

Domini .uk, .co.uk, .me.uk e .org.uk

Se si sta trasferendo un dominio .uk,. co.uk,. me.uk o. org.uk a Route 53, non è necessario ottenere un codice di autorizzazione. Puoi invece utilizzare il metodo fornito dal registrar del dominio attuale per aggiornare il valore del tag IPS per il dominio a GANDI, tutte lettere maiuscole. (Un tag IPS è richiesto da Nominet, il record per i nomi di dominio .uk.) Se il registrar non fornisce un modo per modificare il valore del tag IPS, contatta Nominet.

Tieni presente quanto segue in relazione alla modifica del tag IPS:

È necessario richiedere il trasferimento entro cinque giorni

Se non richiedi il trasferimento entro cinque giorni dalla modifica del tag IPS, il tag torna al valore precedente. È necessario modificare nuovamente il valore del tag IPS o la richiesta di trasferimento non riuscirà.

Visualizzazione del tag IPS nelle query WHOIS

La modifica apportata al tag IPS non viene visualizzata nelle query WHOIS fino al completamento del trasferimento a Route 53.

E-mail da Gandi

Potresti ricevere un'e-mail dal nostro registrar associato, Gandi, in relazione al processo di trasferimento. Se si riceve un'e-mail da Gandi (transfer-auth@gandi.net) in relazione trasferimento del dominio, ignorare le istruzioni contenute nell'e-mail perché non sono pertinenti a Route 53. Segui invece le istruzioni in questo argomento.

Rinnova la registrazione del dominio prima di trasferire il dominio (area geografica selezionata) TLDs

Nella maggior parte dei casi TLDs, quando trasferisci un dominio, la registrazione viene automaticamente estesa di un anno. Tuttavia, per alcune aree geografiche TLDs, la registrazione non viene estesa quando si trasferisce il dominio. Se stai trasferendo su Route 53 un dominio con uno di questi TLDs, ti consigliamo di rinnovare la registrazione del dominio prima di trasferire il dominio, soprattutto se la data di scadenza si avvicina.

> **Important**
>
> Se non vuoi rinnovare il dominio prima di trasferirlo, la registrazione potrebbe scadere prima che il trasferimento sia completo. In questo caso, il dominio non è più disponibile su Internet e il nome di dominio potrebbe diventare disponibile per l'acquisto da parte di altri utenti.

La registrazione non viene automaticamente estesa quando si trasferiscono i seguenti domini in un altro registrar:

- .ch (Svizzera)
- .cl (Cile)

- .co.uk (Regno Unito)
- .co.za (Sudafrica)
- .com.au (Australia)
- .cz (Repubblica Ceca)
- .es (Spagna)
- .fi (Finlandia)
- .im (Isola di Man)
- .jp (Japan)
- .me.uk (Regno Unito)
- .net.au (Australia)
- .org.uk (Regno Unito)
- .se (Sweden)
- .uk (United Kingdom)

Fase 4: Ottieni i nomi dei server dei nomi

Se si utilizza Amazon Route 53 come servizio DNS o se si continua a utilizzare il servizio DNS esistente, i nomi dei server di nomi saranno ottenuti automaticamente in un secondo momento. Passa a Fase 5: Richiedi il trasferimento.

Se si desidera modificare il servizio DNS con un provider diverso da Route 53 nello stesso momento in cui si trasferisce il dominio a Route 53, utilizzare la procedura fornita dal provider di servizi DNS per ottenere i nomi dei server di nomi per ogni nome di dominio che si desidera trasferire.

> **Important**
>
> Se il registrar per il dominio è anche il provider di servizi DNS del dominio, è necessario trasferire il servizio DNS a Route 53 o a un altro provider di servizi DNS prima di continuare con il processo di trasferimento della registrazione del dominio.
> Se trasferisci il servizio DNS nello stesso momento in cui trasferisci la registrazione del dominio, il tuo sito Web, le e-mail e le applicazioni Web associate al dominio potrebbero diventare non disponibili. Per ulteriori informazioni, consulta Fase 2 (facoltativa): trasferisci il tuo servizio DNS ad Amazon Route 53 o a un altro provider di servizi DNS.

Fase 5: Richiedi il trasferimento

Per il trasferimento della registrazione del dominio dal registrar attuale ad Amazon Route 53, utilizzare la console Route 53. Route 53 gestisce la comunicazione con il registrar corrente del dominio.

Puoi utilizzare la console per trasferire fino a cinque domini.

La procedura da seguire dipende se desideri trasferire un singolo dominio o fino a cinque domini:

- Trasferimento della registrazione di un dominio singolo a Route 53
- Come trasferire la registrazione di dominio a Route 53 per un massimo di cinque domini

Segui la procedura Trasferisci il dominio sul tuo account per trasferire un singolo dominio sul tuo account.

Trasferimento della registrazione di un dominio singolo a Route 53

1. Apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Nella pagina Domini registrati seleziona Dominio singolo dal menu a discesa Trasferisci in.
4. Nella pagina Trasferisci dominio sul tuo account, nella sezione Controlla la trasferibilità del dominio inserisci il nome del dominio di cui desideri trasferire la registrazione a Route 53 e seleziona Controlla.
5. Se la registrazione del dominio è disponibile per il trasferimento, verifica di aver completato i requisiti di trasferimento per i domini di primo livello e seleziona Avanti.

   Se la registrazione del dominio non è disponibile per il trasferimento, la console Route 53 riporta i motivi. Contatta il tuo registrar per informazioni su come risolvere i problemi che impediscono di trasferire la registrazione.
6. Nella pagina Servizio DNS controlla le informazioni sui name server e seleziona Avanti.
7. Se richiesto, inserisci il codice di autorizzazione o il tag IPS ricevuto dal tuo attuale registrar in Fase 3: Modifica delle impostazioni con il registrar corrente.

> **Note**
>
> Non è necessario inserire un codice di autorizzazione per trasferire un dominio.co.za, .uk, .co.uk, .me.uk o.org.uk su Route 53.

Scegli Next (Successivo).

8. Nella pagina Opzioni prezzo dominio, scegli il numero di anni per cui desideri registrare il dominio che stai trasferendo e se vuoi che la registrazione del dominio sia rinnovata automaticamente prima della data di scadenza.

> **Note**
>
> Le registrazioni dei nomi di dominio e i rinnovi non sono rimborsabili. Se si abilita il rinnovo automatico del dominio e si decide che non si vuole il nome del dominio dopo il rinnovo della registrazione, non è possibile ottenere un rimborso per il costo del rinnovo.

Scegli Next (Successivo).

9. Nella pagina Informazioni di contatto, inserisci le informazioni di contatto del registrante del dominio, dell'amministratore, dei contatti tecnici e di fatturazione. I valori inseriti in questa pagina vengono applicati a tutti i domini che stai registrando. Per ulteriori informazioni, consulta Valori specificati durante la registrazione o il trasferimento di un dominio.

   Tieni presente le considerazioni seguenti:

   Nome e cognome

   Per First Name (Nome) e Last Name (Cognome), consigliamo di specificare il nome indicato nel tuo documento di identità ufficiale. Per alcune modifiche alle impostazioni di dominio, alcuni record di dominio richiedono di fornire una prova di identità. Il nome sul tuo ID deve corrispondere al nome del registrant per il dominio.

   Contatti diversi

   Per impostazione predefinita, utilizziamo le stesse informazioni per tutte e tre i contatti. Se desideri inserire informazioni diverse per uno o più contatti, imposta su off il toggle Uguale al registrant.

> **Note**
>
> Per i domini .it, i contatti del registrant e dell'admin devono corrispondere.

Informazioni obbligatorie aggiuntive

Per alcuni domini di primo livello (TLDs), siamo tenuti a raccogliere informazioni aggiuntive. Per questi TLDs, inserisci i valori applicabili dopo il campo Codice postale/CAP.

Protezione della privacy

Scegli se desideri nascondere le informazioni di contatto dalle query WHOIS.

> **Note**
>
> È necessario specificare la stessa impostazione di privacy dei contatti dell'admin, del registranti e del tecnico.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio
- Domini che è possibile registrare con Amazon Route 53

> **Note**
>
> Per attivare la protezione della privacy per i domini .uk, .me.uk e .org.uk, è necessario aprire una pratica di supporto e richiedere la protezione della privacy.

Scegli Next (Successivo).

10. Nella pagina Rivedi, controlla le informazioni che hai inserito e, se lo desideri, correggile. Leggi i termini di servizio e seleziona la casella di controllo per confermare di aver letto i termini del servizio.

    Scegliere Submit request (Invia richiesta).

11. Nel pannello di navigazione, seleziona Domini, quindi Richieste.

    In questa pagina puoi visualizzare lo stato del dominio e anche se è necessario rispondere all'e-mail di verifica del contatto del registrant. Puoi anche decidere di inviare nuovamente l'e-mail di verifica.

    Se per il contatto del registrant hai specificato un indirizzo e-mail che non è mai stato utilizzato per registrare un dominio con Route 53, alcuni registri TLD richiedono di verificare che l'indirizzo sia valido.

    Inviamo un'e-mail di verifica da uno dei seguenti indirizzi e-mail:

    - noreply@registrar.amazon — per la TLDs registrazione presso Amazon Registrar.
    - noreply@domainnameverification.net — per la registrazione TLDs effettuata dal nostro registrar associato, Gandi. Per stabilire chi è il registrar per il tuo TLD, consulta Ricerca del registrar.

    > **Important**
    >
    > Il registrant deve seguire le istruzioni nell'e-mail per verificare che l'e-mail è stata ricevuta oppure dobbiamo sospendere il dominio, secondo quanto stabilito da ICANN. Quando un dominio è sospeso, non è accessibile da Internet.

    a. Quando ricevi l'e-mail di verifica, scegli il collegamento nell'e-mail che verifica se l'indirizzo e-mail è valido. Se non ricevi l'e-mail immediatamente, controlla la cartella di posta indesiderata.
    b. Torna alla pagina Richieste. Se lo stato non si aggiorna automaticamente per indicare email-address is verified (l'indirizzo e-mail è verificato), scegli Refresh status (Aggiorna stato).

12. Quando il trasferimento del dominio è completo, la fase successiva varia in base al tipo di servizio che intendi utilizzare, Route 53 o un altro servizio DNS come servizio DNS per il dominio:

    - Route 53: nella hosted zone che Route 53 ha creato quando hai registrato il dominio, crea i record per indicare a Route 53 come desideri instradare il traffico per il dominio e i sottodomini.

      Ad esempio, quando un utente inserisce il tuo nome di dominio in un browser e la query viene inoltrata a Route 53, vuoi che Route 53 risponda alla query con l'indirizzo IP di un server

Web nel tuo data center o con il nome di un sistema di bilanciamento del carico Elastic Load Balancing?

Per ulteriori informazioni, consulta Utilizzo dei record.

> **Important**
>
> Se crei record in una zona ospitata diversa da quella creata automaticamente da Route 53, è necessario aggiornare i server di nomi affinché il dominio li utilizzi per la nuova zona ospitata.

- Un altro servizio DNS: configura il tuo nuovo dominio per instradare le query DNS all'altro servizio DNS. Esegui la procedura Come aggiornare i name server per utilizzare un altro registrar.

Attieniti alla seguente procedura per trasferire fino a cinque domini sul tuo account.

Come trasferire la registrazione di dominio a Route 53 per un massimo di cinque domini

1. Apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Nella pagina Domini registrati seleziona Domini multipli dal menu a discesa Trasferisci in.
4. Nella pagina Trasferisci più domini sul tuo account inserisci massimo cinque domini da trasferire e il relativo codice di autorizzazione, se richiesto, per riga, e seleziona Verifica.
5. Se è disponibile per il trasferimento, la registrazione del dominio viene mostrata nell'elenco di Disponibilità dei domini come disponibile. Seleziona la casella di controllo accanto ad ogni dominio di cui intendi trasferire la registrazione, verifica di aver completato i requisiti di trasferimento per i domini di primo livello e seleziona Avanti.

   Se la registrazione del dominio non è disponibile per il trasferimento, la console Route 53 riporta i motivi. Contatta il tuo registrar per informazioni su come risolvere i problemi che impediscono di trasferire la registrazione.
6. Nella pagina Servizio DNS controlla le informazioni sui name server e seleziona Avanti.

> **Note**
>
> Le registrazioni e i rinnovi dei nomi di dominio non sono rimborsabili. Se si abilita il rinnovo automatico del dominio e si decide che non si vuole il nome del dominio dopo il rinnovo della registrazione, non è possibile ottenere un rimborso per il costo del rinnovo.

7. Nella pagina Informazioni di contatto inserisci le informazioni di contatto relative al registrant del dominio, all'admin e al tecnico. I valori inseriti in questa pagina vengono applicati a tutti i domini che stai trasferendo.

> **Important**
>
> Si consiglia di specificare i seguenti valori per il contatto del registrante (il proprietario del dominio):
>
> - Nome e cognome: suggeriamo di specificare il nome indicato nel documento di identità ufficiale. Per alcune modifiche alle impostazioni di dominio, alcuni record di dominio richiedono di fornire una prova di identità. Il nome sul tuo ID deve corrispondere al nome del registrant per il dominio.
> - Dettagli di contatto: durante il trasferimento del dominio, si consiglia di specificare gli stessi valori specificati con il registrar attuale. Quando si modificano i dettagli di contatto per il contatto del registrant, si modifica il proprietario del dominio e alcuni record TLD non consentono di modificare il proprietario del dominio durante un trasferimento di dominio. Se si modificano i dettagli di contatto per il contatto del registrant, il trasferimento potrebbe non andare a buon fine. È possibile modificare i dettagli di contatto per il contatto del registrant dopo aver trasferito il dominio.

Per impostazione predefinita, utilizziamo le stesse informazioni per tutte e tre i contatti. Se desideri inserire informazioni diverse per uno o più contatti, imposta su off il valore Uguale al registrant.

> **Note**
>
> Per i domini .it, i contatti del registrant e dell'admin devono corrispondere.

Per ulteriori informazioni, consulta Valori specificati durante la registrazione o il trasferimento di un dominio.

8. Per alcuni TLDs, siamo tenuti a raccogliere informazioni aggiuntive. Per questi TLDs, inserisci i valori applicabili dopo il campo Codice postale/CAP.
9. Se il valore di Contact Type (Tipo contatto) è Person (Persona), scegliere se nascondere le informazioni del contatto dalle query WHOIS. Per ulteriori informazioni, consulta Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio.
10. Scegli Invia.
11. Esamina le informazioni inserite, leggi i termini di servizio e seleziona la casella di controllo per confermare di aver letto i termini del servizio.
12. Scegliere Submit request (Invia richiesta).

    Confermiamo che i domini sono idonei per il trasferimento, e inviamo un'e-mail ai contatti del registrant per il dominio per richiedere l'autorizzazione a trasferire il dominio.
13. Nel pannello di navigazione, seleziona Domini, quindi Richieste.

    In questa pagina puoi visualizzare lo stato del dominio e anche se è necessario rispondere all'e-mail di verifica del contatto del registrant. Puoi anche decidere di inviare nuovamente l'e-mail di verifica.

    Se per il contatto del registrant hai specificato un indirizzo e-mail che non è mai stato utilizzato per registrare un dominio con Route 53, alcuni registri TLD richiedono di verificare che l'indirizzo sia valido.

    Inviamo un'e-mail di verifica da uno dei seguenti indirizzi e-mail:

    - noreply@registrar.amazon — per la TLDs registrazione presso Amazon Registrar.
    - noreply@domainnameverification.net — per la registrazione TLDs effettuata dal nostro registrar associato, Gandi. Per stabilire chi è il registrar per il tuo TLD, consulta Ricerca del registrar.

> **Important**
>
> Il registrant deve seguire le istruzioni nell'e-mail per verificare che l'e-mail è stata ricevuta oppure dobbiamo sospendere il dominio, secondo quanto stabilito da ICANN. Quando un dominio è sospeso, non è accessibile da Internet.

a. Quando ricevi l'e-mail di verifica, scegli il collegamento nell'e-mail che verifica se l'indirizzo e-mail è valido. Se non ricevi l'e-mail immediatamente, controlla la cartella di posta indesiderata.

b. Torna alla pagina Richieste. Se lo stato non si aggiorna automaticamente per indicare email-address is verified (l'indirizzo e-mail è verificato), scegli Refresh status (Aggiorna stato).

14. Quando il trasferimento del dominio è completo, la fase successiva varia in base al tipo di servizio che intendi utilizzare, Route 53 o un altro servizio DNS come servizio DNS per il dominio:

- Route 53: nella hosted zone che Route 53 ha creato quando hai registrato il dominio, crea i record per indicare a Route 53 come desideri instradare il traffico per il dominio e i sottodomini.

  Ad esempio, quando un utente inserisce il tuo nome di dominio in un browser e la query viene inoltrata a Route 53, desideri che Route 53 risponda alla query con l'indirizzo IP di un server Web nel tuo data center o con il nome di un load balancer ELB?

  Per ulteriori informazioni, consulta Utilizzo dei record.

  > **Important**
  >
  > Se crei record in una zona ospitata diversa da quella creata automaticamente da Route 53, è necessario aggiornare i server di nomi affinché il dominio li utilizzi per la nuova zona ospitata.

- Un altro servizio DNS: configura il tuo nuovo dominio per instradare le query DNS all'altro servizio DNS. Esegui la procedura Come aggiornare i name server per utilizzare un altro registrar.

Fase 6: Fai clic sul link contenuto nelle e-mail di conferma e autorizzazione

Subito dopo richiesto il trasferimento, invieremo una o più e-mail al contatto del registrant per il dominio:

E-mail per confermare la raggiungibilità del contatto del registrant

Se non è mai stato registrato un dominio con Route 53 né è mai stato trasferito, invieremo un'e-mail di conferma della validità dell'indirizzo e-mail. Conserviamo queste informazioni in modo da non dover inviare nuovamente l'e-mail di conferma.

E-mail per ottenere l'autorizzazione per trasferire il dominio

Per alcuni TLDs, è necessario rispondere a un'e-mail per autorizzare il trasferimento del dominio.

Generici TLDs come .com, .net e.org

L'autorizzazione non è necessaria per i domini che hanno un TLD generico, ad esempio .com, .net o .org.

Geografico TLDs , ad esempio .co.uk e.jp

Per i domini che hanno un TLD geografico, dobbiamo ottenere la tua autorizzazione al trasferimento del dominio. Se trasferisci 10 domini, dobbiamo inviarti 10 e-mail e tu devi fare clic sul link di autorizzazione in ciascuna di esse.

Tutte le e-mail arrivano al contatto del registrant del dominio:

- Se sei tu il registrant, segui le istruzioni contenute nell'e-mail per autorizzare il trasferimento.
- Se qualcun altro è il registrant, chiedi a tale persona di seguire le istruzioni contenute nell'e-mail per autorizzare il trasferimento.

> **Important**
>
> Se intendi trasferire un dominio che ha un TLD geografico, attendiamo fino a cinque giorni che il contatto del registrant autorizzi il trasferimento. Se il registrant non risponde entro cinque giorni, annulliamo l'operazione di trasferimento e inviamo un'e-mail circa l'annullamento.

Argomenti

E-mail di autorizzazione per un nuovo proprietario o indirizzo e-mail

Se hai modificato i seguenti valori, ti invieremo un'e-mail a parte per richiedere l'autorizzazione:

Proprietario del dominio

Se modifichi il proprietario del dominio, come illustrato in Chi è il proprietario di un dominio?, invieremo una e-mail al registrant per il dominio.

Indirizzo e-mail per il contatto del registrante (solo per alcuni) TLDs

Per alcuni TLDs, se modifichi l'indirizzo e-mail del contatto del registrante, inviamo un'e-mail al vecchio e al nuovo indirizzo e-mail di contatto del registrante. Qualcuno per entrambi gli indirizzi e-mail deve seguire le istruzioni nell'e-mail per autorizzare la modifica.

Per le modifiche al proprietario del dominio o all'indirizzo e-mail del registrant, se non riceviamo l'autorizzazione alla modifica entro 3-15 giorni, a seconda del dominio di primo livello, dobbiamo annullare la richiesta, secondo quanto stabilito da ICANN.

Indirizzi e-mail dai quali provengono le e-mail di autorizzazione

Tutte le e-mail provengono da uno dei seguenti indirizzi e-mail.

TLDs	Indirizzo e-mail dal quale proviene l'autorizzazione
.com.au e .net.au	no-reply@ispapi.net L'e-mail contiene un link all'indirizzo http://transfers.ispapi.net.
.fr	nic@nic.fr, se modifichi il contatto del registrant per un nome di dominio.fr nello stesso momento in cui trasferisci il dominio. (L'e-mail viene inviata sia al vecchio registrant, sia al nuovo.)

TLDs	Indirizzo e-mail dal quale proviene l'autorizzazione
Tutti gli altri	Uno dei seguenti indirizzi e-mail: • noreply@registrar.amazon • noreply@domainnameverification.net

Per stabilire chi è il registrar per il tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

Approvazione dal registrar attuale

Se il registrant autorizza il trasferimento, iniziamo a lavorare con il tuo attuale registrar per trasferire il tuo dominio. Questa operazione potrebbe richiedere fino a dieci giorni, a seconda del TLD per il tuo dominio:

- Domini di primo livello generici: impiega fino a sette giorni
- Domini di primo livello geografici (noto anche come domini di primo livello con codice paese): impiega fino a dieci giorni

Se il tuo attuale registrar non risponde alla nostra richiesta di trasferimento, cosa che accade spesso con i registrar, il trasferimento avviene automaticamente. Se il tuo attuale registrar respinge la richiesta di trasferimento, invieremo una notifica tramite e-mail all'attuale contatto del registrant. Il registrant deve contattare l'attuale registrar e risolvere i problemi con il trasferimento.

Cosa succede dopo

Quando il trasferimento del dominio è stato approvato, invieremo un'altra e-mail al contatto del registrant. Per ulteriori informazioni sul processo, consulta Visualizzazione dello stato di un trasferimento di dominio.

Addebitiamo il costo del trasferimento del dominio sul tuo AWS account non appena il trasferimento è completo. Per un elenco dei costi di ogni TLD, consultare Prezzi di Amazon Route 53 per la registrazione dei domini.

> **Note**
>
> Si tratta di un addebito una tantum, quindi l'addebito non viene visualizzato nelle metriche di CloudWatch fatturazione. Per ulteriori informazioni sui CloudWatch parametri, consulta Using Amazon CloudWatch metrics nella Amazon CloudWatch User Guide.

Passaggio 7: aggiorna la configurazione del dominio

Una volta completato il trasferimento, puoi modificare le impostazioni seguenti:

Blocco del trasferimento

Per trasferire il dominio a Route 53, il blocco del trasferimento è stato disabilitato. Se desideri riabilitare il blocco per impedire trasferimenti non autorizzati, consulta Blocco di un dominio per evitare il trasferimento non autorizzato a un altro registrar.

Rinnovo automatico

Configuriamo il dominio trasferito per il rinnovo automatico con l'avvicinarsi della data di scadenza. Per informazioni su come modificare questa impostazione, consulta Abilitazione o disabilitazione del rinnovo automatico per un dominio.

Periodo di registrazione esteso

Per impostazione predefinita, Route 53 rinnova il dominio ogni anno. Se desideri registrare il dominio per un periodo di tempo più lungo, consulta Estendere il periodo di registrazione per un dominio.

DNSSEC

Per ulteriori informazioni sulla configurazione di DNSSEC per il dominio, consulta Configurazione di DNSSEC per un dominio.

Visualizzazione dello stato di un trasferimento di dominio

Una volta avviato il trasferimento di un dominio da un altro registrar di dominio ad Amazon Route 53, puoi monitorarne lo stato dalla pagina Richieste (nuova console) o dalla pagina Richieste in sospeso (vecchia console) della console Route 53. La colonna Status (Stato) include una breve descrizione della fase corrente. L'elenco seguente include il testo nella console e una descrizione più dettagliata di ciascuna fase.

> **Note**
>
> Quando invii una richiesta di trasferimento, lo stato iniziale è Domain transfer request submitted (Richiesta di trasferimento dominio ricevuta), che indica che abbiamo ricevuto la tua richiesta.

Determinare se il dominio soddisfa i requisiti di trasferimento (fase 1 di 14)

Stiamo confermando che lo stato del tuo dominio è idoneo per il trasferimento. Devi sbloccare il tuo dominio e il dominio non può avere uno dei seguenti codici di stato quando invii la richiesta di trasferimento:

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

TLDs Solo area geografica: verifica delle informazioni WHOIS (fase 2 di 14)

Se intendi trasferire un dominio che ha un TLD geografico, inviamo una query WHOIS per il dominio per stabilire se hai disabilitato la protezione della privacy. Se la protezione della privacy è ancora abilitata con il tuo attuale registrar, non saremo in grado di accedere alle informazioni necessarie per trasferire il dominio.

> **Note**
>
> L'autorizzazione non è necessaria per i domini che hanno un TLD generico, ad esempio .com, .net o .org.

TLDs Solo area geografica: e-mail inviata al contatto del registrante per ottenere l'autorizzazione al trasferimento (fase 3 di 14)

Se intendi trasferire un dominio che ha un TLD geografico, abbiamo inviato un'e-mail al contatto del registrant per il dominio. Lo scopo dell'e-mail è quello di ricevere conferma che il trasferimento è stato richiesto da un contatto autorizzato del dominio.

> **Note**
>
> L'autorizzazione non è necessaria per i domini che hanno un TLD generico, ad esempio .com, .net o .org.

Verifica del trasferimento con l'attuale registrar (fase 4 di 14)

Abbiamo inviato una richiesta all'attuale registrar per il dominio per avviare il trasferimento.

TLDs Solo area geografica: in attesa dell'autorizzazione da parte del contatto del registrante (fase 5 di 14)

Abbiamo inviato un'e-mail al registrant per il dominio (vedi la fase 3 di 14) e siamo in attesa che faccia clic su un link nell'e-mail per autorizzare il trasferimento. Se intendi trasferire un dominio che ha un TLD geografico e per qualche motivo non hai ricevuto la e-mail, consulta Rinvio di e-mail di autorizzazione e di conferma.

Contattato il registrar corrente per richiedere il trasferimento (fase 6 di 14)

Stiamo lavorando con l'attuale registrar per il dominio per completare il trasferimento.

In attesa che l'attuale registrar completi il trasferimento (fase 7 di 14)

Il tuo attuale registrar sta confermando che il tuo dominio soddisfa i requisiti per il trasferimento. Questa operazione potrebbe richiedere fino a dieci giorni, a seconda del TLD per il tuo dominio:

- Domini di primo livello generici: impiega fino a sette giorni
- Domini di primo livello geografici (noto anche come domini di primo livello con codice paese): impiega fino a dieci giorni

> **Note**
>
> Se hai approvato l'e-mail di conferma inviata da Route 53 durante il trasferimento di un dominio .JP, ma è interrotta per diversi giorni nel passaggio 7, contatta Centro assistenza AWS per ricevere assistenza.

Per la maggior dei registrar, il processo è completamente automatico e non può essere accelerato. Alcuni registra inviano un'e-mail che richiede di approvare il trasferimento; se il tuo registrar invia questa e-mail di conferma, il processo di trasferimento potrebbe essere molto più veloce rispetto a sette-dieci giorni.

Per informazioni sui motivi per cui un registrar potrebbe rifiutare il trasferimento, consulta Requisiti per il trasferimento dei domini di primo livello.

Conferma con il registrant che il contatto che ha iniziato il trasferimento (fase 8 di 14)

Alcuni record TLD inviano un'altra e-mail al registrant per confermare che il trasferimento del dominio è stato richiesto da un utente autorizzato.

Sincronizzazione dei server dei nomi con il record (fase 9 di 14)

Questo passaggio viene eseguito solo se i server dei nomi che hai fornito nell'ambito della richiesta di trasferimento sono diversi dai server dei nomi che sono indicati con l'attuale registrar. Cercheremo di aggiornare i tuoi nomi dei server con i nuovi server dei nomi che hai fornito.

Sincronizzazione delle impostazioni con il record (fase 10 di 14)

Stiamo verificato che il trasferimento sia stato completato e stiamo sincronizzando i dati relativi al dominio con il nostro registrar.

Invio di dati di contatto aggiornati al record (fase 11 di 14)

Se hai modificato il proprietario del dominio quando hai richiesto il trasferimento, stiamo tentando di applicare questa modifica. Tuttavia, la maggior parte dei record non consente un trasferimento di proprietà nell'ambito del processo di trasferimento di dominio.

Finalizzazione del trasferimento a Route 53 (fase 12 di 14)

Stiamo confermando che il processo di trasferimento sia stato eseguito correttamente.

Finalizzazione del trasferimento (fase 13 di 14)

Stiamo configurando il dominio in Route 53.

Trasferimento completo (fase 14 di 14)

Il trasferimento è stato completato correttamente.

Come il trasferimento di un dominio ad Amazon Route 53 influenza la data di scadenza della registrazione del dominio

Quando trasferisci un dominio da un registrar a un altro, alcuni record consentono di mantenere la stessa data di scadenza per il dominio, alcuni record aggiungono un anno dalla data di scadenza e alcuni record modificano la data di scadenza a un anno dopo la data di trasferimento.

> **Note**
>
> Nella maggior parte dei casi TLDs, è possibile estendere il periodo di registrazione di un dominio fino a dieci anni dopo il trasferimento su Amazon Route 53. Per ulteriori informazioni, consulta Estendere il periodo di registrazione per un dominio.

Generico TLDs

Quando si esegue il trasferimento di un dominio con un TLD generico (ad esempio, .com) a Route 53, la nuova data di scadenza per il dominio sarà la data di scadenza scelta con il registrar precedente, più un anno.

Geografico TLDs

Quando si esegue il trasferimento di un dominio con un TLD geografico (per esempio, .co.uk) a Route 53, la nuova data di scadenza per il dominio dipende dal TLD. Trova il TLD nella tabella seguente per determinare in che modo il trasferimento del tuo dominio interessa la data di scadenza.

Continente	Geografia TLDs ed effetto del trasferimento di un dominio alla data di scadenza
Africa	.co.za: la data di scadenza rimane invariata.
Americhe	.cl, .com.ar, .com.br: la data di scadenza rimane invariata. .ca, .co, .mx, .us: viene aggiunto un anno alla data di scadenza precedente.
Asia/Oceania	.co.nz, .com.au, .com.sg, .jp, .net.au, .net.nz, .org.nz, .ru, .sg: la data di scadenza rimane invariata. .in: viene aggiunto un anno alla data di scadenza precedente.
Europa	.ch, .co.uk, .de, .es, .fi, .me.uk, .org.uk, .se: la data di scadenza rimane invariata.

Continente	Geografia TLDs ed effetto del trasferimento di un dominio alla data di scadenza
	.berlin, .eu, .io, .me, .ruhr, .wien: viene aggiunto un anno alla data di scadenza precedente. .be, .fr, .it, .nl: la nuova data di scadenza è un anno dopo la data del trasferimento.

Trasferimento di un dominio su un altro account AWS

Se hai registrato un dominio utilizzando un AWS account e desideri trasferire il dominio su un altro AWS account, puoi trasferirlo facilmente utilizzando la nuova console o utilizzando gli AWS CLI o altri metodi programmatici.

Argomenti

- Passaggio 1: trasferire un dominio su un altro account AWS
- Passaggio 2 (facoltativo): migra una zona ospitata su un altro account AWS

Passaggio 1: trasferire un dominio su un altro account AWS

I domini non possono essere trasferiti entro i primi 14 giorni dalla registrazione.

Quando avvii il trasferimento di un dominio, devi accedere utilizzando l'account root o tramite un utente a cui sono state concesse le autorizzazioni IAM in uno o più dei seguenti modi:

- All'utente viene assegnata la policy AdministratorAccessgestita.
- All'utente viene assegnata la policy DomainsFullAccess gestita AmazonRoute53.
- All'utente viene assegnata la politica FullAccess gestita AmazonRoute53.
- All'utente viene assegnata la politica PowerUserAccessgestita.
- L'utente ha l'autorizzazione per eseguire tutte le seguenti operazioni: `TransferDomains`, `DisableDomainTransferLock` e `RetrieveDomainAuthCode`.

Se non accedi utilizzando l'account root o un utente in possesso delle autorizzazioni necessarie, non saremo in grado di operare il trasferimento. Questo requisito impedisce agli utenti non autorizzati di trasferire domini ad altri. Account AWS

Il processo di trasferimento prevede due fasi. Innanzitutto il proprietario dell'account di origine avvia il trasferimento nella procedura avvia un trasferimento su un altro Account AWS, quindi il proprietario dell'account di destinazione accetta il trasferimento nella procedura accetta un trasferimento da un altro Account AWS.

Per trasferire un dominio su un altro account AWS

1. Accedi AWS utilizzando il nome su Account AWS cui è attualmente registrato il dominio.
2. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
4. Seleziona il nome del dominio che intendi trasferire su un altro Account AWS.
5. Sopra la sezione Dettagli, nel menu a discesa Trasferimento in uscita, scegli Trasferisci su un altro Account AWS.
6. Nella finestra di dialogo Trasferisci su un altro Account AWS, inserisci l'ID dell'account di destinazione. Puoi ottenere questo ID dal proprietario dell' Account AWS di destinazione.
7. Scegli Conferma.
8. Nella finestra di dialogo Genera password, copia la password e inoltrala al Account AWS proprietario ricevente.

   Nella pagina Richieste, sullo Stato del dominio verrà visualizzato In corso e su Tipo verrà visualizzato Trasferimento interno in uscita.

Per accettare il trasferimento di un dominio da un altro AWS account

1. Accedi AWS utilizzando il nome Account AWS che sta ricevendo il dominio.
2. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione seleziona Richieste.
4. Nella pagina Richieste, seleziona il pulsante di opzione accanto al nome di dominio che stai trasferendo da un altro Account AWS. Se il dominio è pronto per essere trasferito, sullo Stato verrà visualizzata Azione obbligatoria e su tipo verrà visualizzato Trasferimento interno del dominio.

   Hai a disposizione tre giorni per accettare la richiesta. Se il trasferimento non viene accettato entro tre giorni, la richiesta di trasferimento viene annullata.
5. Dal menu a discesa Azione seleziona Accetta.

Puoi anche selezionare Rifiuta per annullare il processo di trasferimento.

6. Se hai accettato, nella pagina Trasferisci il dominio sul tuo account, nella sezione Password inserisci la password ricevuta dal proprietario dell'account di origine.

   Accetta i termini e le condizioni e seleziona Seguente.

7. Vai alla pagina Richieste per monitorare lo stato del trasferimento e gli altri passaggi da completare.
8. Una volta completato il trasferimento, puoi aggiornare le informazioni di contatto. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto e di proprietà per un dominio.

Come trasferire il dominio programmaticamente

Puoi anche trasferire il dominio a livello di codice utilizzando l'API Route 53 AWS CLI, uno dei o l' AWS SDKsAPI Route 53. Per ulteriori informazioni, consulta la seguente documentazione :

- Per una panoramica del processo di trasferimento e la documentazione sulle azioni API utilizzate per trasferire un dominio utilizzando l'API di registrazione del dominio Route 53, consulta TransferDomainToAnotherAwsAccountAmazon Route 53 API Reference.
- Per la documentazione su altre opzioni per il trasferimento di domini a livello di codice, consulta "SDKs & Toolkits» nella sezione Guide e riferimenti API della pagina "documentazione».AWS
- L'account ricevente ha tre giorni per accettare il trasferimento dall'account di origine, utilizzando l'API -aws-account. transfer-domain-to-another Se il trasferimento non viene accettato entro tre giorni, la richiesta di trasferimento viene annullata.

> **Important**
>
> Quando trasferisci un dominio su un altro AWS account, la zona ospitata per il dominio non viene trasferita. Se vuoi trasferire la zona ospitata, attendi il trasferimento del dominio, quindi consulta Passaggio 2 (facoltativo): migra una zona ospitata su un altro account AWS.

Passaggio 2 (facoltativo): migra una zona ospitata su un altro account AWS

Se si utilizza Route 53 come servizio DNS per il dominio, Route 53 non trasferisce le zone ospitate quando si trasferisce un dominio a un account attuale AWS diverso. Se la registrazione di dominio

è associata a un account e la zona ospitata corrispondente è associata a un altro account, né la registrazione del dominio né la funzionalità DNS sono interessate. L'unico effetto è che è necessario effettuare l'accesso alla console Route 53 utilizzando un account per visualizzare il dominio ed effettuare l'accesso utilizzando l'altro account per visualizzare la zone ospitata.

Se si è il proprietario dell'account da cui si sta trasferendo il dominio e dell'account a cui lo si sta trasferendo, è possibile decidere di migrare la zona ospitata del dominio a un account diverso, ma non è obbligatorio. Route 53 continuerà a utilizzare i record nella zona ospitata esistente per instradare il traffico per il dominio.

> **Important**
>
> Se non possiedi sia l'account da cui stai trasferendo il dominio sia l'account verso cui trasferisci il dominio, devi migrare la zona ospitata esistente all' AWS account verso cui stai trasferendo il dominio o creare una nuova zona ospitata in un AWS account di tua proprietà. Se non sei proprietario dell'account che ha creato la zona ospitata che instrada il traffico per il dominio, non puoi controllare le modalità di instradamento del traffico.

Per migrare la zona ospitata esistente al nuovo account, consulta Migrazione di una zona ospitata su un altro account AWS.

Per creare una nuova zona ospitata, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente. Questo argomento viene in genere utilizzato quando si trasferiscono domini da un altro registrar a Route 53, ma il processo è lo stesso quando si trasferiscono domini da un AWS account a un altro.

Trasferimento di un dominio da Amazon Route 53 a un altro registrar

Quando si esegue il trasferimento di un dominio da Amazon Route 53 a un altro registrar, Route 53 invia alcune informazioni che dovranno essere fornite al nuovo registrar. Il nuovo registrar farà il resto.

> **Important**
>
> Se al momento si utilizza Route 53 come provider di servizi DNS e si desidera trasferire il servizio DNS a un altro provider, le seguenti funzionalità di Route 53 non dispongono di paralleli diretti con le funzionalità offerte da altri provider di servizi DNS. Devi lavorare con il nuovo fornitore di servizi DNS per determinare come ottenere funzionalità equivalenti:

- Record di alias. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.
- Policy di routing diverse dalla policy di routing semplice. Per ulteriori informazioni, consulta Scegliere una policy di routing.
- Controlli di stato associati ai record. Per ulteriori informazioni, consulta Configurazione di un failover DNS.

La maggior parte dei registrar di domini applicano requisiti specifici sul trasferimento di un dominio a un altro registrar. Lo scopo principale di questi requisiti è impedire ai proprietari di domini fraudolenti di trasferire ripetutamente i domini a diversi registrar. I requisiti variano, ma i seguenti sono generalmente comuni:

- È necessario aver registrato il dominio presso il registrar corrente o trasferito la registrazione del dominio al registrar corrente almeno 14 giorni fa.
- Il dominio non può avere uno dei seguenti codici di stato del nome di dominio:
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - serverTransferProhibited

Per un elenco aggiornato dei codici di stato dei nomi di dominio e una spiegazione del significato di ciascun codice, visita il sito Web ICANN e cerca epp status codes (codici di stato EPP). (Consigliamo di eseguire la ricerca sul sito web dell'ICANN; talvolta le ricerche sul Web restituiscono una vecchia versione del documento).

> **Note**
>
> Se desideri trasferire il tuo dominio a un altro registrar di domini ma l' AWS account con cui è registrato il dominio è chiuso, sospeso o chiuso, puoi contattare il AWS Supporto per ricevere assistenza. I domini non possono essere trasferiti entro i primi 14 giorni dalla registrazione. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

> **Note**
>
> Se il nuovo registrar richiede un codice REG-ID, puoi contattare Support per ricevere AWS assistenza. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Come trasferire un dominio da Route 53 a un altro registrar

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Seleziona il nome del dominio che desideri trasferire a un altro registrar.
4. Nella pagina nome dominio controlla il valore di Codice di stato nome dominio. Se si tratta di uno dei seguenti valori, non attualmente non puoi trasferire il dominio:

   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - clientTransferProhibited
   - serverTransferProhibited

   Per un elenco aggiornato dei codici di stato dei nomi di dominio e una spiegazione del significato di ciascun codice, visita il sito Web ICANN e cerca epp status codes (codici di stato EPP). (Consigliamo di eseguire la ricerca sul sito web dell'ICANN; talvolta le ricerche sul Web restituiscono una vecchia versione del documento).

   Se il valore del codice di stato del nome di dominio è serverTransferProhibited, puoi contattare l' AWS assistenza gratuitamente per sapere cosa devi fare per trasferire il dominio. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.
5. Se il valore di Blocco trasferimento è impostato su Attivo, selezionaDisattiva blocco trasferimento dal menu a discesa Azioni.

> **Note**
>
> Contatta l' AWS assistenza per sbloccare il trasferimento dei domini.jp da parte del registrar. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

6. Tutti i domini tranne i domini.be, .co.za, .ru, .uk, .co.uk, .me.uk e .org.uk: nella pagina del nome del dominio, scegli Trasferisci a un altro registrar dal menu a discesa Trasferisci in uscita.

   Nella finestra di dialogo Trasferisci a un altro registrar seleziona Copia per copiare il codice di autorizzazione per il trasferimento del dominio. Dovrai fornire questo valore ai tuoi registrar più avanti in questa procedura.

   > **Note**
   >
   > Per i domini.eu, puoi anche generare il codice di autenticazione utilizzando il pannello «My.eu» nel registro: https://my.eurid.eu/.

   Domini.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk e .org.uk: procedi come segue:

   domini.be

   Ottieni il codice di autorizzazione dal registro per i domini.be sul sito Web DNS Belgio.

   Domini .co.za

   Non è necessario ottenere un codice di autorizzazione per trasferire una. co.za dominio in un altro registrar.

   Domini .ru

   Ottieni il codice di autorizzazione dal registro per i domini.ru all'indirizzo https://www.nic. ru/en/auth/recovery/:

   a. Scegliere l'opzione per recuperare le credenziali per nome di dominio.
   b. Immettere il nome di dominio e scegliere Continue (Continua).
   c. Seguire le istruzioni visualizzate per ottenere l'accesso alla pagina di amministrazione RU-CENTER.

d. Nella sezione Manage your account (Gestisci account), scegliere Domain transfer (Trasferimento del dominio).

e. Confermare il trasferimento con REGRU-RU.

Domini .uk, .co.uk, .me.uk e .org.uk

Modificare il tag IPS nel valore per il nuovo registrar:

a. Andare alla pagina Find a Registrar (Trova un registrar) sul sito Web di Nominet e individuare il tag IPS per il nuovo registrar. (Nominet è il record per i domini .uk,. co.uk,. me.uk e. org.uk.)

b. Nella pagina Domini registrati > nome di dominio, seleziona il menu a discesa Trasferisci in uscita, quindi Aggiorna tag IPS e specifica il valore ottenuto al passaggio 6a.

c. Scegli Aggiorna.

> **Note**
>
> Puoi anche aggiornare il tag IPS sulla console Nominet. Per istruzioni, consulta Cambia il registrar.

7. Se al momento non si utilizza Route 53 come provider di servizi DNS per il proprio dominio, passare alla fase 10.

   Se si utilizza Route 53 come fornitore di servizi DNS per il dominio, completare la seguente procedura:

   a. Scegli Hosted Zones (Zone ospitate).

   b. Selezionare il nome della zona ospitata per il dominio. Il dominio e la zona ospitata hanno lo stesso nome.

   c. Se si desidera continuare a utilizzare Route 53 come provider di servizi DNS per il dominio: ottenere i nomi dei quattro server dei nomi che Route 53 ha assegnato alla zona ospitata. Per ulteriori informazioni, consulta Ottenere i server di nomi per una zona ospitata pubblica.

      Se non si desidera continuare a utilizzare Route 53 come provider di servizi DNS per il dominio: prendere nota delle impostazioni per tutti i tuoi record eccetto NS e SOA. Per le caratteristiche specifiche di Route 53, ad esempio i record alias, è necessario lavorare con il nuovo provider di servizi DNS per determinare il modo in cui ottenere funzionalità equivalenti.

8. Se si trasferisce un servizio DNS a un altro provider, utilizzare i metodi che vengono forniti tramite il nuovo servizio DNS per eseguire le attività seguenti:

   - Creare una zona ospitata
   - Creazione di record che riproducono la funzionalità dei record Route 53
   - Ottieni il server dei nomi che il nuovo servizio DNS ha assegnato alla zona ospitata

9. Utilizza il processo che viene fornito dal nuovo registrar per richiedere un trasferimento del dominio.

   Tutti i domini tranne i domini.co.za, .uk, .co.uk, .me.uk e .org.uk: ti verrà richiesto di inserire il codice di autorizzazione ottenuto dalla console Route 53 nel passaggio 6 di questa procedura.

10. Se desideri comunque utilizzare Route 53 come provider di servizi DNS, utilizza la procedura fornita dal nuovo registrar per specificare i nomi dei name server Route 53 che hai ottenuto al passaggio 7. Se desideri utilizzare un altro provider di servizi DNS, specifica i nomi dei name server che il nuovo provider ti ha fornito quando hai creato una nuova zona ospitata nel passaggio 8.

11. Rispondere all'e-mail di conferma:

    Tutti i domini tranne i domini .jp

    Route 53 invia un'e-mail di conferma all'indirizzo e-mail del registrant per il dominio:

    - Se non rispondi a questa e-mail, il trasferimento avviene automaticamente nella data specificata.
    - Se si desidera che il trasferimento avvenga prima o se si desidera annullare il trasferimento, selezionare il link contenuto nel messaggio e-mail per accedere al sito Web di Route 53 e selezionare l'opzione applicabile.
    - A seconda del TLD, l'e-mail di conferma può contenere un link al https://approvemove.com quale è possibile approvare o rifiutare il trasferimento. Quando la protezione della privacy è abilitata per i contatti del dominio, l'e-mail verrà recapitata dagli indirizzi identity-protect.org per i contatti registrati TLDs presso Amazon Registrar. Per stabilire chi è il registrar per il tuo TLD, consulta Ricerca del registrar.

    Domini .jp

    Route 53 invia un'e-mail di conferma all'indirizzo e-mail del contatto del registrant per il dominio dall'indirizzo noreply@domainnameverification.net con un link per confermare il trasferimento:

- Se non si risponde a questa e-mail, il trasferimento avverrà automaticamente alla data specificata.
- Se si desidera che il trasferimento avvenga prima o se si desidera annullare il trasferimento, selezionare il link contenuto nel messaggio e-mail per accedere al sito Web di Route 53 e selezionare l'opzione applicabile. Ti verrà richiesto di fornire il codice di autorizzazione del dominio ottenuto nella fase 7.

Inoltre, è possibile che venga ricevuta un'e-mail da Wixi.jp. È possibile ignorare questa e-mail.

12. Se il registrar cui si sta trasferendo il dominio segnala che il trasferimento non è riuscito, contatta tale registrar per ulteriori informazioni. Quando si trasferisce un dominio in un altro registrar, tutti gli aggiornamenti di stato passano al nuovo registrar, pertanto Route 53 non dispone di informazioni sul perché un trasferimento non è riuscito.

    Se il nuovo registrar segnala che il trasferimento non è riuscito perché il codice di autorizzazione ricevuto da Route 53 non è valido, apri una controversia con AWS Support. (Non è necessario un contratto di assistenza e non esistono costi aggiuntivi.) Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

    > **Note**
    >
    > I codici di autorizzazione generati da Gandi sono validi per circa 5 giorni. Se il tentativo di trasferimento avviene dopo questo periodo, potrebbe fallire a causa di un codice scaduto.

13. Se il servizio DNS è stato trasferito a un altro provider di servizi DNS, è possibile eliminare i record nella zona ospitata ed eliminare la zona ospitata dopo che i resolver DNS smettono di rispondere alle query DNS con i nomi dei server di nomi Route 53. Questo di solito richiede due giorni, la quantità di tempo per cui i resolver DNS comunemente memorizzano nella cache i nomi dei server di nomi per un dominio.

    > **Important**
    >
    > Se si elimina la zona ospitata mentre i resolver DNS stanno ancora rispondendo alle query DNS con i nomi dei server di nomi Route 53, il dominio diventerà non disponibile su Internet.

Una volta eliminata la zona ospitata, Route 53 interromperà la fatturazione della tariffa mensile per una zona ospitata. Per ulteriori informazioni, consulta la seguente documentazione :

- Eliminazione di record
- Eliminazione di una zona ospitata pubblica
- Prezzi di Route 53

Trasferimento da un registrar ad Amazon Registrar

Amazon Route 53 Domains utilizza due registrar per registrare i domini per i clienti: Amazon Registrar, un registrar di proprietà e gestito da, e Gandi AWS, un registrar associato con cui collaboriamo. Inizialmente, la maggior parte dei domini Route 53 erano registrati tramite Gandi perché Amazon Registrar non era accreditato direttamente per molti domini di primo livello (TLDs), come.com o.club. Ora che Amazon Registrar è accreditato direttamente presso centinaia di domini TLDs (e in crescita), inizieremo a trasferire i domini registrati tramite Gandi ad Amazon Registrar per tuo conto.

Ciò non cambierà il modo in cui gestisci il dominio all'interno di Route 53, ma aggiornerà semplicemente il registrar di record per il tuo dominio da Gandi ad Amazon Registrar. Il trasferimento avverrà durante il processo di rinnovo del dominio e verrà applicata solo la tariffa di rinnovo standard. Una volta completato il trasferimento, le nuove richieste di trasferimento del dominio a un nuovo registrar esterno AWS potrebbero subire ritardi. Route 53 informerà i registranti del dominio interessati 15 giorni prima del trasferimento in merito al rinnovo. Questa procedura è descritta nel nostro Contratto di registrazione dei nomi di dominio (vedere la sezione 3.11.5).

Questo trasferimento è obbligatorio se desideri continuare a utilizzare il servizio Route 53 per gestire i tuoi domini. Se non desideri utilizzare Amazon Registrar per gestire il tuo dominio, dovrai trasferire il dominio a un altro registrar entro 15 giorni dalla ricezione dell'avviso di trasferimento al momento del rinnovo da. AWS

Rinvio di e-mail di autorizzazione e di conferma

Per diverse operazioni correlate alla registrazione di dominio, ICANN richiede di ottenere l'autorizzazione dal registrant per il dominio o la conferma che l'indirizzo e-mail di contatto del registrant sua valido. Per ottenere l'autorizzazione o conferma, inviamo un'e-mail contenente un link.

Hai tra 3 e 15 giorni per fare clic sul collegamento, a seconda dell'operazione e del dominio di primo livello. Dopodiché, il collegamento smette di funzionare.

Se non fai clic sul link contenuto nel messaggio e-mail nell'intervallo di tempo specificato ICANN generalmente richiede di sospendere il dominio o annullare l'operazione, a seconda delle operazioni che si cercano di fare:

Registrazione di un dominio

Sospendiamo il dominio, in modo che non sia accessibile su Internet. Per inviare di nuovo l'e-mail di conferma, consulta Per inviare di nuovo l'e-mail di conferma della registrazione per un dominio.

TLDs Solo geografico: trasferimento di un dominio su Amazon Route 53

Se intendi trasferire un dominio che ha un TLD geografico, annulliamo il trasferimento. Per inviare di nuovo l'e-mail di autorizzazione, consulta Per inviare di nuovo l'e-mail di autorizzazione per il trasferimento di un dominio.

> **Note**
>
> L'autorizzazione non è necessaria per i domini che hanno un TLD generico, ad esempio .com, .net o .org.

Cambiare il nome o l'indirizzo e-mail del registrant per il dominio (il proprietario)

Annulliamo la modifica. Per inviare di nuovo l'e-mail di autorizzazione, consulta Per inviare di nuovo l'e-mail di autorizzazione per aggiornare il contatto del registrant o eliminare un dominio.

Eliminazione di un dominio

Annulliamo la richiesta di eliminazione. Per inviare di nuovo l'e-mail di autorizzazione, consulta Per inviare di nuovo l'e-mail di autorizzazione per aggiornare il contatto del registrant o eliminare un dominio.

TLDs Solo geografico: trasferisci un dominio da Route 53 a un altro registrar

Se intendi trasferire un dominio che ha un TLD geografico, il nuovo registrar annulla il trasferimento.

> **Note**
>
> L'autorizzazione non è necessaria per i domini che hanno un TLD generico, ad esempio .com, .net o .org.

Argomenti

Aggiornamento degli indirizzi e-mail

Inviamo sempre e-mail di conferma e autorizzazione all'indirizzo e-mail per il registrant di un dominio. Per alcuni TLDs, siamo tenuti a inviare e-mail al vecchio e al nuovo indirizzo e-mail di contatto del registrante nei seguenti casi:

- Stai modificando l'indirizzo e-mail per un dominio che è già registrato con Amazon Route 53.
- Stai modificando l'indirizzo e-mail per un dominio che stai trasferendo a Route 53

Rinvio di e-mail

Utilizza la procedura applicabile per inviare e-mail di conferma o di autorizzazione.

- Per inviare di nuovo l'e-mail di conferma della registrazione per un dominio
- Per inviare di nuovo l'e-mail di autorizzazione per il trasferimento di un dominio
- Per inviare di nuovo l'e-mail di autorizzazione per aggiornare il contatto del registrant o eliminare un dominio

Per inviare di nuovo l'e-mail di conferma della registrazione per un dominio

1. Controlla l'indirizzo e-mail per il registrant e, se necessario, aggiornala. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto e di proprietà per un dominio.
2. Controlla la cartella spam nella tua applicazione per un'e-mail da uno dei seguenti indirizzi e-mail.

Se è passato troppo tempo, il link non funziona più, ma potrai sapere dove cercare l'e-mail di conferma quando te ne invieremo un'altra.

TLDs	Indirizzo e-mail da cui proviene l'e-mail di conferma o di approvazione
.fr	nic@nic.fr
Tutti gli altri	Uno dei seguenti indirizzi e-mail: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Le e-mail potrebbero contenere un link a www.verify-whois.com. Questo link si può utilizzare in tutta sicurezza.

3. Utilizza la console Amazon Route 53 per inviare di nuovo l'e-mail di conferma:

   a. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   b. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).

   c. Seleziona il nome del dominio per cui desideri inviare nuovamente l'e-mail.

   d. Nella casella di avviso con l'intestazione "Il tuo dominio potrebbe essere sospeso", selezionare Send email again (Invia e-mail di nuovo).

   > **Note**
   >
   > Se non c'è una casella di avviso, hai già confermato che l'indirizzo e-mail di contatto per il registrant è valido.

4. Se riscontri problemi durante il reinvio dell'e-mail di conferma, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Per inviare di nuovo l'e-mail di autorizzazione per il trasferimento di un dominio

Questo metodo non funziona per le richieste di trasferimento del dominio .jp.

1. Utilizzare il metodo fornito dall'attuale registrar del dominio per confermare che la protezione della privacy per il dominio è disattivata. In caso contrario, disabilitarla.

   Inviamo l'e-mail di autorizzazione all'indirizzo e-mail che l'attuale registrar ha salvato nel database WHOIS. Quando è abilitata la protezione della privacy, questo indirizzo e-mail in genere è offuscato. Il registrar corrente potrebbe non inoltrare al tuo indirizzo e-mail effettivo l'e-mail che Amazon Route 53 invia all'indirizzo e-mail nel database WHOIS.

   > **Note**
   >
   > Se l'attuale registrar del dominio non ti consente di disabilitare la protezione della privacy, possiamo comunque trasferire il dominio se hai specificato un codice di autorizzazione valido in Fase 5: Richiedi il trasferimento.

2. Controlla l'indirizzo e-mail per il registrant e, se necessario, aggiornala. Utilizza il metodo fornito dall'attuale registrar per il dominio.
3. Controlla la cartella spam nella tua applicazione per un'e-mail da uno dei seguenti indirizzi e-mail.

   Se è passato troppo tempo, il link non funziona più, ma potrai sapere dove cercare l'e-mail di autorizzazione quando te ne invieremo un'altra.

TLDs	Indirizzo e-mail da cui proviene l'e-mail di conferma o di approvazione
.com.au e .net.au	no-reply@ispapi.net L'e-mail contiene un collegamento a. https://approve.domainadmin.com
.fr	

TLDs	Indirizzo e-mail da cui proviene l'e-mail di conferma o di approvazione
	nic@nic.fr
Tutti gli altri	Uno dei seguenti indirizzi e-mail: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Le e-mail potrebbero contenere un link a www.verify-whois.com. Questo link si può utilizzare in tutta sicurezza.

4. Se il trasferimento non è più in corso (se lo abbiamo già annullato perché è passato troppo tempo), richiedere il trasferimento di nuovo, e invieremo un'e-mail di autorizzazione.

> **Note**
>
> Per i primi 15 giorni dopo la richiesta di un trasferimento, è possibile determinare lo stato del trasferimento selezionando la tabella Notifiche nella pagina Pannello di controllo nella console Route 53. Dopo 15 giorni, usa il AWS CLI per ottenere lo stato. Per ulteriori informazioni, consulta route53domains in Riferimento ai comandi AWS CLI .

Se il trasferimento è ancora in corso, esegui la procedura seguente per inviare nuovamente l'e-mail di autorizzazione.

a. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

b. Nella tabella Notifiche, individua il dominio da trasferire.

c. Nella colonna Status (Stato) del dominio, selezionare Resend email (Invia nuovamente e-mail).

5. Se riscontri problemi durante il reinvio dell'e-mail di autorizzazione per il trasferimento di un dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Per inviare di nuovo l'e-mail di autorizzazione per aggiornare il contatto del registrant o eliminare un dominio

1. Controlla l'indirizzo e-mail per il registrant e, se necessario, aggiornala. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto e di proprietà per un dominio.
2. Controlla la cartella spam nella tua applicazione per un'e-mail da uno dei seguenti indirizzi e-mail.

   Se è passato troppo tempo, il link non funziona più, ma potrai sapere dove cercare l'e-mail di autorizzazione quando te ne invieremo un'altra.

TLDs	Indirizzo e-mail dal quale proviene l'autorizzazione
.fr	nic@nic.fr
Tutti gli altri	Uno dei seguenti indirizzi e-mail: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> Le e-mail potrebbero contenere un link a www.verify-whois.com. Questo link si può utilizzare in tutta sicurezza.

3. Annullare la modifica o l'eliminazione. Sono disponibili due opzioni:

   - Puoi attendere da 3 a 15 giorni, dopodiché annulliamo automaticamente l'operazione richiesta.
   - In alternativa, puoi contattare l' AWS assistenza e chiedere loro di annullare l'operazione.

4. Dopo che l'eliminazione o la modifica viene annullata, è possibile modificare le informazioni di contatto o eliminare il dominio nuovamente, e ti invieremo un'e-mail di autorizzazione.
5. Se riscontri problemi durante il reinvio dell'e-mail di autorizzazione, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Configurazione di DNSSEC per un dominio

Alcuni malintenzionati talvolta dirottano il traffico verso gli endpoint Internet come ad es. i server Web intercettando query DNS e restituendo i propri indirizzi IP ai resolver DNS al posto dell'indirizzo IP effettivo per quegli endpoint. Gli utenti vengono quindi instradati agli indirizzi IP forniti dagli aggressori nella risposta di spoofing, ad esempio a siti Web falsi.

Puoi proteggere il tuo dominio da questo tipo di attacco, noto come spoofing o man-in-the-middle attacco DNS, configurando Domain Name System Security Extensions (DNSSEC), un protocollo per proteggere il traffico DNS.

> **Important**
>
> Amazon Route 53 supporta la firma DNSSEC e DNSSEC per la registrazione del dominio. Se desideri configurare la firma DNSSEC per un dominio registrato con Route 53, consulta Configurazione della firma DNSSEC in Amazon Route 53.

Argomenti

- Panoramica di come DNSSEC protegge i domini
- Prerequisiti e valori massimi per la configurazione di DNSSEC per un dominio
- Aggiunta di chiavi pubbliche a un dominio
- Eliminazione di chiavi pubbliche per un dominio

Panoramica di come DNSSEC protegge i domini

Quando configuri DNSSEC per il tuo dominio, un resolver DNS stabilisce una catena di certificati per le risposte provenienti da resolver intermedi. La catena di attendibilità inizia con il record TLD per il dominio (la zona padre del dominio) e termina con il server di nomi autorevole presso il tuo

fornitore di servizi DNS. Non tutti i resolver DNS supportano DNSSEC. Solo i resolver che supportano DNSSEC possono eseguire la convalida di firme o di autenticità.

Ecco come configurare il protocollo DNSSEC per i domini registrati con Amazon Route 53, per proteggere gli host Internet dallo spoofing DNS, semplificato per maggiore chiarezza:

1. Utilizzare il metodo fornito dal provider di servizi DNS per firmare i record nella zona ospitata con la chiave privata in una coppia di chiavi asimmetrica.

   > **Important**
   >
   > Route 53 supporta la firma DNSSEC e DNSSEC per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

2. Fornire la chiave pubblica dalla coppia di chiavi al registrar di dominio e specificare l'algoritmo utilizzato per generare la coppia di chiavi. Il registrar di dominio inoltra la chiave pubblica e l'algoritmo di record per il dominio di primo livello (TLD).

   Per informazioni su come eseguire questa operazione per i domini che hai registrato con Route 53, consulta Aggiunta di chiavi pubbliche a un dominio.

Dopo aver configurato DNSSEC, ecco come protegge il tuo dominio dallo spoofing DNS:

1. Invia una query DNS, ad esempio, navigando su un sito Web o inviando un messaggio e-mail.
2. La richiesta viene instradata a un resolver DNS. I resolver sono responsabili del ripristino del valore appropriato ai client in base alla richiesta, ad esempio l'indirizzo IP dell'host che esegue un server Web o un server di posta elettronica.
3. Se l'indirizzo IP viene memorizzato nella cache del resolver DNS perché qualcun altro ha già inviato la stessa query DNS e il resolver ha già ottenuto il valore, il resolver restituisce l'indirizzo IP al client che ha inviato la richiesta. Il client utilizza quindi l'indirizzo IP per accedere all'host.

   Se l'indirizzo IP non viene memorizzato nella cache del resolver DNS, il resolver invia una richiesta alla zona padre per il dominio, presso il record TLD, che restituisce due valori:

   - Il record Delegation Signer (DS), che è una chiave pubblica che corrisponde alla chiave privata utilizzata per firmare il record.
   - Gli indirizzi IP dei server di nomi ufficiali per il tuo dominio.

4. Il resolver DNS invia la richiesta originale a un altro resolver DNS. Se il resolver non contiene l'indirizzo IP, ripete il processo fino a quando un resolver invia la richiesta a un server di nomi presso il tuo fornitore di servizi DNS. Il server di nomi restituisce due valori:
   - I record per il dominio, ad esempio esempio.com. In genere questo contiene l'indirizzo IP di un host.
   - La firma per il record, che è stato creato quando hai configurato DNSSEC.
5. Il resolver DNS utilizza la chiave pubblica che hai fornito al registrar di dominio e che il registrar ha inoltrato al record TLD per eseguire due operazioni:
   - Stabilire una catena di attendibilità.
   - Verificare che la risposta firmata dal fornitore di servizi DNS è legittima e non è stata sostituita con una risposta negativa da parte di un malintenzionato.
6. Se la risposta è autentica, il resolver restituisce il valore al client che ha inviato la richiesta.

   Se la risposta non può essere verificata, il resolver lo segnala tramite errore all'utente.

   Se il record TLD del dominio non dispone della chiave pubblica per il dominio, il resolver risponde alla query DNS utilizzando la risposta ottenuta dal fornitore di servizi DNS.

Prerequisiti e valori massimi per la configurazione di DNSSEC per un dominio

Per configurare DNSSEC per un dominio, il dominio e il fornitore di servizi DNS devono soddisfare i seguenti prerequisiti:

- Il record per il TLD deve supportare DNSSEC. Per determinare se il record per il tuo TLD supporta DNSSEC, consulta Domini che è possibile registrare con Amazon Route 53.
- Il fornitore di servizi DNS per il dominio deve supportare DNSSEC.

> **Important**
>
> Route 53 supporta la firma DNSSEC e DNSSEC per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

- È necessario configurare DNSSEC con il provider di servizi DNS per il dominio prima di aggiungere le chiavi pubbliche per il dominio a Route 53.

- Il numero di chiavi pubbliche che è possibile aggiungere a un dominio dipende dal TLD per il dominio:
  - Domini .com e .net: fino a tredici chiavi
  - Tutti gli altri domini: fino a quattro chiavi

Aggiunta di chiavi pubbliche a un dominio

Quando si ruotano le chiavi o si abilita DNSSEC per un dominio, eseguire la seguente procedura dopo aver configurato DNSSEC con il fornitore di servizi DNS per il dominio.

Per aggiungere chiavi pubbliche per un dominio

1. Se non hai già configurato DNSSEC presso il tuo fornitore di servizi DNS, utilizza il metodo fornito dal provider di servizi per configurare DNSSEC.
2. Accedi e apri la console Route 53 all'indirizzo. AWS Management Console https://console.aws.amazon.com/route53/
3. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
4. Seleziona il nome del dominio a cui desideri aggiungere chiavi.
5. Seleziona la scheda Chiavi DNSSEC e seleziona Aggiungi chiave.
6. Specifica i seguenti valori:

   Tipo di chiavi

   Scegli se preferisci caricare una chiave per l'identificazione della chiave (KSK) o una chiave per l'identificazione della zona (ZSK).

   Algoritmo

   Scegli l'algoritmo utilizzato per firmare il record per le hosted zone.

   Chiavi pubbliche

   Specifica la chiave pubblica dalla coppia di chiavi asimmetrica utilizzata per configurare DNSSEC con il tuo fornitore di servizi DNS.

   Tieni presente quanto segue:

   - Specificare la chiave pubblica, non il file digest.
   - È necessario specificare la chiave in formato base64.

7. Scegli Aggiungi.

> **Note**
>
> Puoi aggiungere solo una chiave pubblica per volta. Se hai bisogno di aggiungere ulteriori chiavi, attendi finché non ricevi un'e-mail di conferma da Route 53.

8. Quando Route 53 riceve una risposta dal record, invieremo un'e-mail al registrant di dominio. L'e-mail conferma che la chiave pubblica è stata aggiunta al dominio sul record o spiega perché non è stato possibile aggiungere la chiave.

Eliminazione di chiavi pubbliche per un dominio

Quando si ruotano le chiavi o si disabilita DNSSEC per il dominio, elimina le chiavi pubbliche utilizzando la seguente procedura prima di disabilitare DNSSEC presso il provider di servizi DNS. Tieni presente quanto segue:

- Se stai ruotando la chiave pubblica, ti consigliamo di attendere fino a tre giorni dopo aver aggiunto la nuova chiave pubblica per eliminare la vecchia chiave.
- Se stai disabilitando DNSSEC, elimina prima le chiavi pubbliche per il dominio. Ti consigliamo di attendere fino a tre giorni prima di disabilitare DNSSEC con il servizio DNS per il dominio.

> **Important**
>
> Se DNSSEC è abilitato per il dominio e disabiliti DNSSEC presso il servizio DNS, i resolver DNS che supportano DNSSEC restituiranno un errore `SERVFAIL` ai client e questi non saranno in grado di accedere agli endpoint associati al dominio.

Per eliminare chiavi pubbliche per un dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Seleziona il nome del dominio da cui desideri eliminare chiavi.

4. Nella scheda Chiavi DNSSEC, seleziona il pulsante di opzione accanto alla chiave da eliminare, quindi seleziona Elimina chiave.
5. Nella finestra di dialogo Elimina chiave DNSSEC, inserisci delete nella casella di testo per confermare che desideri eliminare la chiave, quindi seleziona Elimina.

> **Note**
>
> Puoi eliminare solo una chiave pubblica per volta. Se hai bisogno di eliminare ulteriori chiavi, attendi finché non ricevi un'e-mail di conferma da Amazon Route 53.

6. Quando Route 53 riceve una risposta dal record, invieremo un'e-mail al registrant di dominio. L'e-mail conferma che la chiave pubblica è stata eliminata dal dominio sul record o spiega perché non è stato possibile eliminare la chiave.

Ricerca del registrar e altre informazioni sul tuo dominio

Per visualizzare le informazioni sul dominio utilizzando l'GetDomainDetailAPI, puoi utilizzare una delle opzioni SDKs o AWS CLI. Per ulteriori informazioni, consulta get-domain-detail.

Visualizzazione delle informazioni sui domini con la CLI di **`get-domain-detail`**

- Utilizza il seguente comando della CLI:

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> Questo comando viene eseguito solo in us-east-1 Regione AWS.

Tutte le informazioni sul tuo dominio, inclusi il registrar, la data di registrazione, le impostazioni sulla privacy e così via, saranno riportate nell'output.

Visualizzazione delle informazioni sui domini registrati con Route 53

Puoi visualizzare le informazioni sui domini registrati tramite Route 53. Queste informazioni includono dettagli come quando il dominio è stato originariamente registrato e le informazioni di contatto del proprietario del dominio e per i contatti tecnici, amministrativi e di fatturazione.

WHOIS

WHOIS è una directory gratuita e disponibile al pubblico contenente informazioni sui domini sponsorizzati dai registrar e dai registri di domini. Viene fornito sia come servizio che accetta richieste sulla porta 43, sia come sito Web, entrambi IPv4 accessibili tramite e. IPv6 WHOIS è una ricerca gerarchica distribuita. Per ulteriori informazioni, consulta Informazioni su WHOIS.

Una richiesta WHOIS a diversi livelli della gerarchia può fornire diverse informazioni:

- Una richiesta al root WHOIS (whois.iana.org) fornisce informazioni sul registro.
- Una richiesta al registro WHOIS fornisce informazioni sul registrar e alcune informazioni pubbliche sul dominio.
- Una richiesta al registrar WHOIS fornisce tutte le informazioni pubbliche sul dominio.

Poiché esistono più livelli di WHOIS, incluse le ricerche WHOIS gestite dal registro TLD e dal registrar di dominio, la disattivazione della protezione della privacy sulla console Route 53 è possibile solo sul WHOIS fornito dal registrar. Alcuni registri mantengono di proposito servizi di protezione della privacy o di redazione per i propri servizi di ricerca WHOIS a prescindere dal fatto che tu li abbia disattivati con Route 53. Per ottenere informazioni complete sul tuo dominio, è consigliabile utilizzare il WHOIS fornito dal registrar.

Tieni presente quanto segue:

E-mail ai contatti del dominio quando è abilitata la protezione della privacy

> Se per il dominio è abilitata la protezione della privacy, le informazioni di contatto del registrant, e dei contatti tecnici e amministrativi vengono sostituite con le informazioni di contatto del servizio di privacy di Amazon Registrar. Ad esempio, se il dominio example.com è registrato con Amazon Registrar e se la protezione della privacy è abilitata, il valore di E-mail registrant nella risposta a una query WHOIS dovrebbe essere simile a owner1234@example.com.identity-protect.org.

Per contattare uno o più contatti di dominio quando è abilitata la protezione della privacy, inviare un'e-mail agli indirizzi e-mail corrispondenti. Inoltreremo automaticamente la tua e-mail al contatto applicabile.

Segnalazione di usi illeciti

Per segnalare qualsiasi attività illegale o violazione della Politica d'uso accettabile, inclusi contenuti inappropriati, phishing, malware o spam, invia un'e-mail a trustandsafety@support.aws.com.

Come visualizzare informazioni sui domini registrati con Route 53

1. In un browser Web, accedi a uno dei seguenti siti Web:
   - Amazon Registrar WHOIS: /whois https://registrar.amazon.com
   - Amazon Registrar RDAP: /rdap https://registrar.amazon.com
   - Gandi WHOIS: https://whois.gandi.net
2. Immettere il nome del dominio di cui si desidera visualizzare le informazioni e scegliere Search (Cerca).

Eliminazione della registrazione di un nome di dominio

Per la maggior parte dei domini di primo livello (TLDs), puoi eliminare la registrazione se non la desideri più. Se il record consente di eliminare la registrazione, eseguire la procedura in questo argomento.

Tieni presente quanto segue:

Il costo della registrazione non è rimborsabile

Se elimini la registrazione di un nome di dominio prima della scadenza prevista, AWS non rimborserà la tariffa di registrazione.

TLDs che consentono di eliminare la registrazione di un dominio

Per determinare se puoi eliminare la registrazione per il tuo dominio, consulta Domini che è possibile registrare con Amazon Route 53. Se la sezione del TLD non include una sottosezione "Eliminazione della registrazione di dominio", è possibile eliminare il dominio. Assicurati di disabilitare il blocco del dominio prima di rimuoverlo. Per ulteriori informazioni sulla disabilitazione del blocco del dominio, consulta DisableDomainTransferLock.

Cosa fare se non è possibile eliminare una registrazione di dominio?

Se il record del dominio non consente di eliminare una registrazione del nome di dominio, è necessario attendere la scadenza del dominio. Per garantire che il dominio non venga rinnovato automaticamente, disabilitare il rinnovo automatico del dominio. Dopo la data di scadenza, Route 53 eliminerà automaticamente la registrazione del dominio. Per informazioni su come modificare il rinnovo automatico, consulta Abilitazione o disabilitazione del rinnovo automatico per un dominio.

Ritardo prima dell'eliminazione di un dominio e disponibilità per registrarlo nuovamente.

Quasi tutti i record impediscono di registrare immediatamente un dominio appena scaduto. Il ritardo in genere va da uno a tre mesi, a seconde del TLD. Per ulteriori informazioni, vedi la sezione "Scadenze per il rinnovo e il ripristino dei domini" per il TLD in Domini che è possibile registrare con Amazon Route 53.

> **Important**
>
> Non eliminare un dominio e aspettati di registrarlo nuovamente se desideri semplicemente trasferire il dominio tra AWS account o trasferire il dominio a un altro registrar. Consultare invece la documentazione applicabile:
>
> - Trasferimento di un dominio su un altro account AWS
> - Trasferimento di un dominio da Amazon Route 53 a un altro registrar

Per eliminare la registrazione di un nome di dominio

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
3. Scegli il nome del dominio.

   Se desideri eliminare un dominio .co.uk, .me.uk, .org.uk o .uk, vedi Per eliminare le registrazioni dei nomi di dominio.co.uk, .me.uk, .org.uk e.uk.
4. Se il registro del tuo TLD consente di eliminare una registrazione di nome di dominio, seleziona Elimina dominio.

Per alcuni domini potrebbe essere necessario l'invio, da parte nostra, di un'e-mail al registrant del dominio volta verificare che il registrant desideri eliminare il dominio. Se ricevi un'e-mail, questa verrà inviata da uno dei seguenti indirizzi e-mail:

- noreply@registrar.amazon — per la TLDs registrazione presso Amazon Registrar.
- noreply@domainnameverification.net — per la registrazione TLDs effettuata dal nostro registrar associato, Gandi.

Per stabilire chi è il registrar per il tuo TLD, consulta Domini che è possibile registrare con Amazon Route 53.

5. Quando ricevi l'e-mail di verifica, seleziona il link contenuto nell'e-mail e approva o rifiuta la richiesta di eliminare il dominio.

> **Important**
>
> Il referente del registrante deve seguire immediatamente le istruzioni contenute nell'e-mail, oppure dobbiamo annullare la richiesta di cancellazione non appena dopo un giorno, come richiesto da ICANN.

Riceverai un altro messaggio e-mail quando il dominio è stato eliminato. Per determinare lo stato attuale della tua richiesta, consulta Visualizzazione dello stato di una registrazione di dominio.

6. Elimina i record nella zona ospitata per il dominio eliminato e quindi elimina la zona ospitata. Una volta eliminata la zona ospitata, Route 53 interrompe la fatturazione della tariffa mensile per una zona ospitata. Per ulteriori informazioni, consulta la seguente documentazione :

   - Eliminazione di record
   - Eliminazione di una zona ospitata pubblica
   - Prezzi di Route 53

7. Se riscontri problemi durante l'eliminazione della registrazione di un nome di dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Per eliminare le registrazioni dei nomi di dominio.co.uk, .me.uk, .org.uk e.uk

Se desideri eliminare un dominio.co.uk, .me.uk, .org.uk o .uk, devi creare un account con Nominet, il registro per i domini.uk. Per ulteriori informazioni, vedi la sezione relativa all'annullamento del nome di dominio sul sito Web di Nominet, https://www.nominet.uk/domain-support/.

> **Important**
>
> Se elimini (annulli) un nome di dominio.uk, questo verrà eliminato entro pochi giorni e sarà disponibile per la registrazione da parte di chiunque. Se vuoi solo trasferire il dominio, non eliminarlo.

Ecco una panoramica del processo:

1. Sul sito Web di Nominet, segui le istruzioni per accedere per la prima volta. Per informazioni, consulta https://secure.nominet.org.uk/auth/login.html. Nominet ti invia un'e-mail con le istruzioni per la creazione di una password.
2. Segui le istruzioni contenute nell'e-mail che ricevi da Nominet.
3. Accedi al sito Web di Nominet e segui le istruzioni per annullare (eliminare) un nome di dominio.

Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio

AWS fornisce un piano di assistenza Basic, gratuito, per tutti i AWS clienti. Il piano include assistenza per i seguenti problemi relativi alla registrazione dei domini:

- Trasferimento del dominio da o verso Amazon Route 53
- Trasferimento di domini tra account AWS
- Aumento delle quote relative alle entità Route 53, ad esempio il numero di domini che è possibile registrare (consulta Quote).
- Modifica del proprietario di un dominio
- Modifica delle informazioni di contatto del proprietario di un dominio
- Rinvio di e-mail di autorizzazione e di conferma
- Rinnovo di domini
- Ripristino di domini scaduti

- Recupero di informazioni sulla fatturazione di Route 53
- Presentazione di una prova di identità per i domini .uk
- Eliminazione dei domini o disattivazione del rinnovo automatico dopo la chiusura dell'account AWS

Per contattare l' AWS assistenza in merito a questi e ad altri problemi relativi alla registrazione del dominio, esegui la procedura applicabile.

Argomenti

Contattare AWS l'assistenza quando è possibile accedere al proprio AWS account

Per contattare AWS Support quando riesci ad accedere al tuo AWS account, esegui la seguente procedura:

1. Utilizzando l' AWS account su cui è attualmente registrato il dominio, accedi al AWS Support Center.

   > **Important**
   >
   > Devi firmare utilizzando l'account root a cui il dominio è attualmente registrato. Questo requisito impedisce agli utenti non autorizzati di dirottare il tuo account.

2. Specifica i seguenti valori:

   Regarding (Motivo)

   Accetta il valore predefinito di Account and Billing Support (Supporto per account e fatturazione).

   Servizio

   Accetta il valore predefinito di Domains.

   Categoria

   Accetta il valore predefinito di Registration Issue.

Gravità

Scegli il livello di gravità applicabile:

Subject

Inserisci un breve riepilogo del problema.

Descrizione

Descrivi il problema nel dettaglio e allega tutti i documenti o screenshot utili.

Contact method (Modalità di contatto)

Seleziona come metodo di contatto Web. Ti contatteremo utilizzando l'indirizzo email associato al tuo AWS account.

3. Scegli Invia.

Contattare AWS l'assistenza quando non riesci ad accedere al tuo AWS account

Per contattare AWS Support quando non riesci ad accedere al tuo AWS account, esegui la seguente procedura:

1. Vai alla pagina Sono un AWS cliente e cerco la fatturazione o l'assistenza per l'account.
2. Compila il modulo.
3. Scegli Invia.

Download di un report di fatturazione domini

Se gestisci più domini e desideri visualizzare le tariffe per dominio per un periodo di tempo specificato, puoi scaricare un report di fatturazione del dominio. Questo report include tutte le spese per la registrazione del dominio, tra cui le seguenti:

- Registrazione di un dominio
- Rinnovo della registrazione di un dominio
- Trasferimento di un dominio ad Amazon Route 53
- Cambiare il proprietario di un dominio (per alcuni TLDs, questa operazione è gratuita)

A volte il report di fatturazione può mostrare i periodi di fatturazione futuri. Ciò accade perché il processo di rinnovo automatico del dominio inizia il mese prima della scadenza del dominio. Pertanto, ad esempio, nel rapporto di agosto potresti visualizzare un periodo di fatturazione che inizia a settembre successivo e termina a settembre dell'anno successivo.

Quando si esegue il report utilizzando la console, è possibile scegliere le seguenti opzioni:

- Ultimi 12 mesi: il report include gli addebiti da un anno prima dell'esecuzione del report fino al giorno corrente. Ad esempio, se esegui il report il 3 giugno, questo includerà gli addebiti dal 3 giugno dell'anno precedente fino al giorno corrente.
- Singoli mesi nell'ultimo anno: il report include gli addebiti per il mese specificato.

Se si esegue il report a livello di codice, è possibile ottenere addebiti per qualsiasi intervallo di date a partire dal 31 luglio 2014. Si tratta della data in cui Route 53 ha iniziato a supportare la registrazione del dominio. Ad esempio, consulta view-billing in Riferimento ai comandi AWS CLI .

Il report di fatturazione è in formato CSV e i contenuti sono descritti dall'ViewBillingAPI.

Per il download di un report di fatturazione dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, selezionare Registered Domains (Domini registrati).
3. Scegli Domain billing report (Report di fatturazione domini).
4. Scegli l'intervallo di date per il report e quindi scegli Download domain report (Download del report di dominio).
5. Seguire le istruzioni per aprire o salvare il report.
6. Se riscontri problemi durante il download di un rapporto di fatturazione del dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Domini che è possibile registrare con Amazon Route 53

Important

Puoi utilizzare il servizio DNS di Route 53 con qualsiasi dominio di primo livello scelto e con qualsiasi registrar di domini. Le informazioni in questa pagina riguardano solo i domini che

puoi registrare con Route 53. Per ulteriori informazioni sull'utilizzo di Route 53 come servizio DNS, consulta In che modo il traffico Internet viene instradato al tuo sito o applicazione Web.

I seguenti elenchi di domini di primo livello generici e geografici mostrano i domini di primo livello (TLDs) che puoi utilizzare per registrare domini con Amazon Route 53.

Registrazione di domini con Route 53

I record TLD hanno assegnato prezzi speciali o premium ad alcuni nomi di dominio. Non è possibile utilizzare Route 53 per registrare un dominio che ha un prezzo speciale o premium. I dati TLDs che puoi registrare con Route 53 sono inclusi nei seguenti elenchi. Se il TLD non è incluso, non potrai registrare il dominio con Route 53.

Trasferimento di domini a Route 53

Puoi trasferire un dominio a Route 53 se il TLD è incluso nei seguenti elenchi. Se il TLD non è incluso, non sarà possibile trasferire il dominio a Route 53.

Nella maggior parte dei casi TLDs, è necessario ottenere un codice di autorizzazione dal registrar corrente per trasferire un dominio. Per determinare se hai bisogno di un codice di autorizzazione, consulta la sezione «Codice di autorizzazione richiesto per i trasferimenti» del tuo TLD.

Prezzi per il trasferimento e la registrazione di domini

Per informazioni sul costo per la registrazione o il trasferimento dei domini, consulta Prezzi di Amazon Route 53 per la registrazione di domini.

Utilizzo di Route 53 come servizio DNS

È possibile utilizzare Route 53 come servizio DNS per qualsiasi dominio, anche se il TLD per il dominio non è incluso negli elenchi seguenti. Per ulteriori informazioni sull'utilizzo di Route 53 come servizio DNS, consulta In che modo il traffico Internet viene instradato al tuo sito o applicazione Web. Per informazioni su come trasferire il servizio DNS per il tuo dominio a Route 53, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Nomi di dominio internazionalizzati

Non tutti TLDs supportano i nomi di dominio internazionalizzati (IDNs), ovvero i nomi di dominio che includono caratteri diversi dai caratteri ASCII a-z, 0-9 e - (trattino). L'elenco di ogni TLD indica se tale TLD supporta. IDNs Per ulteriori informazioni sui nomi di dominio internazionalizzati, consulta Formato del nome dominio DNS.

Registrazione di domini geografici con TLDs

Le regole per la registrazione dei dati geografici TLDs variano in base al Paese. Alcuni paesi non prevedono restrizioni, il che significa che chiunque al mondo può registrare tali domini, mentre altri prevedono restrizioni, ad esempio la residenza. L'elenco per ciascun TLD geografico indica eventuali restrizioni.

Indice dei domini di primo livello supportati

Argomenti

Domini di primo livello generici

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, .birra,.bet, .bid, .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, .natale, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .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, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .fun, .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, .legge, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, .ltd

M

.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, .acquisti, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team, .tech,.technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .voto, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .lavoro, .works, .world, .wtf, .xyz, .zone

Domini di primo livello geografici

Africa

.ac (Isola di Ascensione), .co.za (Sudafrica), .sh (Saint Helena)

Americhe

.ca (Canada), .cl (Cile), .co (Colombia), .com.ar (Argentina), .com.br (Brasile), com.mx (Messico), .mx (Messico), .us (Stati Uniti), .vc (Saint Vincent e Grenadine), .vg (Isole Vergini britanniche)

Asia/Oceania

.au (Australia), .cc (Isole Cocos), .co.nz (Nuova Zelanda), .com.au (Australia), .com.sg (Repubblica di Singapore), .fm (Stati Federati di Micronesia), .in (India), .jp (Japan), .io (Territorio britannico dell'Oceano Indiano), .net.au (Australia), .net.nz (Nuova Zelanda), .org.nz (Nuova Zelanda), .pw (Palau), .qa (Qatar), .ru (Federazione russa), .sg (Repubblica di Singapore)

Europa

.be (Belgio), .berlin (città di Berlino in Germania), .ch (Svizzera), .co.uk (Regno Unito), .cz (Repubblica Ceca), .de (Germania), .es (Spagna) , .eu (Unione europea), .fi (Finlandia), .fr (Francia), .gg (Guernsey), .im (Isola di Man), .it (Italia), .me (Montenegro), .me.uk (Regno Unito), .nl (Paesi Bassi), .org.uk (Regno Unito), .ruhr (regione della Ruhr, parte occidentale della Germania), .se (Sweden), .uk (United Kingdom), .wien (città di Vienna in Austria)

Domini di primo livello generici

I domini di primo livello generici (gTLDs) sono estensioni globali utilizzate e riconosciute in tutto il mondo, come.com, .net e.org. Includono anche domini specializzati, come ad esempio .bike, .condos e .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, .birra, .bet, .bid, .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, .natale, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .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, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .fun, .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, .legge, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , .ltd

M

.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, .acquisti, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team,.tech, .technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .voto, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .lavoro, .works, .world, .wtf, .xyz, .zone

.ac

Per informazioni, consulta .ac (Isola di Ascensione).

Return to index

.academy

Utilizzato da istituzioni educative, ad esempio scuole e università. Viene inoltre utilizzato da selezionatori del personale, consulenti, inserzionisti, studenti, insegnanti e amministratori affiliati a istituzioni educative.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.accountants

Utilizzato da aziende, gruppi e individui affiliati alla professione contabile.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.actor

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.adult

Utilizzato per l'hosting di siti Web con contenuti per soli adulti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.agency

Utilizzato da aziende o gruppi che si identificano come agenzie.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.airforce

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.apartments

Utilizzato da agenti immobiliari, proprietari e affittuari.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.associates

Utilizzato da aziende e società che includono il termine "associati" nel loro titoli. Utilizzato anche da gruppi o agenzie che desiderano indicare la natura professionale della propria organizzazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.auction

Utilizzato per eventi correlati ad aste di acquisto e di vendita.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, spagnolo e latino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza

- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.audio

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .audio o trasferire domini .audio a Route 53. Continueremo a supportare i domini .audio che sono già registrati con Route 53.

Utilizzato dall'industria audiovisiva e da chiunque sia interessato a trasmissioni, apparecchiature audio, produzione audio e audio in streaming.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .audio a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.band

Utilizzato per la condivisione di informazioni sulle band e gli eventi delle band. Utilizzato anche dai musicisti per comunicare con i loro fan e vendere il merchandising della band.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, spagnolo e latino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bargains

Utilizzato per informazioni su vendite e promozioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.birra

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bet

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bid

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bike

Utilizzato da aziende o gruppi dedicati a ciclisti, ad esempio negozi di bici, concessionarie di moto e officine.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bingo

Utilizzato per siti Web di giochi online o per la condivisione di informazioni sul gioco del bingo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.bio

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.biz

Utilizzato per uso commerciale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese semplificato, cinese tradizionale, danese, finlandese, tedesco, ungherese, giapponese, coreano, lettone, lituano, norvegese, polacco, portoghese, spagnolo e svedese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.black

Utilizzato da chi ama il nero o da coloro che desiderano associare il colore nero al proprio business o marchio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.blue

Utilizzato da chi ama il blu o da coloro che desiderano associare il colore blu al proprio business o marchio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.boutique

Utilizzato per informazioni su boutique e piccoli negozi specializzati.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.builders

Utilizzato da società e individui affiliati al settore edile.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.business

Utilizzato da qualsiasi tipo di business. Può essere utilizzato come un'alternativa all'estensione .biz.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.buzz

Utilizzato per informazioni sulle ultime novità e gli eventi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per lo spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cab

Utilizzato da società e individui affiliati al settore dei taxi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cafe

Utilizzato da bar e da coloro che hanno interesse nella cultura del caffè.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.camera

Utilizzato da appassionati di fotografia e da chiunque desideri condividere foto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.camp

Utilizzato da parchi e dipartimenti di ricreazione, campeggi estivi, workshop per scrittori, campi fitness e appassionati di campeggio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.capital

Utilizzato come categoria generale che descrive qualsiasi tipo di capitale, ad esempio capitale finanziario o capitale di una città.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cards

Utilizzato da aziende specializzate in carte come ecard, biglietti stampati, biglietti da visita e carte da gioco. Ideale inoltre per i giocatori che vogliono discutere di regole e strategie di giochi di carte.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.care

Utilizzato da aziende o agenzie nel campo dell'assistenza. Utilizzato anche da enti caritativi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.careers

Per informazioni sulle attività di reclutamento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cash

Utilizzato da qualsiasi organizzazione, gruppo o singolo impegnato in attività in materia di denaro.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.casino

Utilizzato dal settore delle scommesse o da giocatori che desiderano condividere informazioni sulle scommesse e i giochi da casinò.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.catering

Utilizzato da aziende nel settore della ristorazione o da coloro che condividono informazioni su eventi correlati al cibo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cc

Per informazioni, consulta .cc (Isole Cocos).

Return to index

.center

Utilizzato come estensione generica per ogni tipo di attività, dalla organizzazioni di ricerca ai centri comunitari.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ceo

Utilizzato per informazioni su CEOs e loro equivalenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per il tedesco.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.chat

Utilizzato da qualsiasi tipo di sito Web di chat online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cheap

Utilizzato dai siti Web di e-commerce per promuovere e vendere prodotti poco costosi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.natale

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 43 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 44 giorni dopo la scadenza
- Il ripristino con il registro è possibile: tra 44 giorni e 86 giorni dopo la scadenza
- Il dominio viene eliminato dal registro: 86 giorni dopo la scadenza

.church

Utilizzato da chiese di qualsiasi dimensione o denominazione per comunicare con la parrocchia e pubblicare informazioni sugli eventi e le attività correlate alla chiesa.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.city

Utilizzato per fornire informazioni su città specifiche, ad esempio i punti di interesse, le cose da vedere o le attività nei quartieri.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.claims

Utilizzato da aziende che gestiscono indennizzi o forniscono servizi di consulenza legale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cleaning

Utilizzato da aziende o individui che forniscono servizi di pulizia.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.click

Utilizzato da aziende che desiderano associare l'azione di clic con i propri siti Web, ad esempio, fare clic su un prodotto su un sito Web per acquistarlo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.clinic

Utilizzato dal settore sanitario e dai medici.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.clothing

Utilizzato da coloro che lavorano nel settore della moda, tra cui rivenditori, grandi magazzini, progettisti, sarti e negozi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cloud

Utilizzato come estensione generale, ma ideale per le aziende che forniscono tecnologie e servizi di cloud computing.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.club

Utilizzato da qualsiasi tipo di club o organizzazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per spagnolo e giapponese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.coach

Utilizzato da coloro che hanno un interesse nel coaching, come i professionisti dello sport, coach di lifestyle o trainer aziendali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.codes

Utilizzato come estensione generica per tutti i tipi di codice, ad esempio codici di condotta, creazione di codici, o codice di programmazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.coffee

Utilizzato da coloro che lavorano nel settore del caffè.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.college

Utilizzato da istituzioni educative, ad esempio scuole e università. Viene inoltre utilizzato da selezionatori del personale, consulenti, inserzionisti, studenti, insegnanti e amministratori affiliati a istituzioni educative.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, cinese semplificato e tradizionale, cirillico, greco, ebraico, giapponese e thai.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.com

Utilizzato per siti Web commerciali. È l'estensione più popolare su Internet.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.community

Utilizzato da qualsiasi tipo di community, club, organizzazione o gruppo di interesse speciale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.company

Utilizzato come estensione generica per aziende di ogni tipo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.computer

Utilizzato come estensione generica per informazioni sui computer.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.condos

Utilizzato da individui e aziende associate a condomini.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.construction

Utilizzato da coloro che lavorano nel settore edile, ad esempio costruttori e appaltatori.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.consulting

Utilizzato da consulenti e altri individui affiliati al settore della consulenza.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, cinese, francese, cirillico, devanagari, tedesco, greco, ebraico, giapponese, coreano, latino, spagnolo, tamil e tailandese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.contact

Utilizzato da chiese di qualsiasi dimensione o denominazione per comunicare con la parrocchia e pubblicare informazioni sugli eventi e le attività correlate alla chiesa.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.contractors

Utilizzato da appaltatori, ad esempio quelli che lavorano nel settore edile.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cool

Utilizzato da organizzazioni e gruppi che desiderano associare il proprio marchio alle ultime tendenze.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.coupons

Utilizzato da produttori e rivenditori che forniscono coupon online e codici di sconto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.credit

Utilizzato dal settore del credito.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.creditcard

Utilizzato da enti o banche che emettono carte di credito.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.cruises

Utilizzato dal settore dei viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.dance

Utilizzato da ballerini, istruttori di danza e scuole di danza.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.dating

Utilizzato per siti Web di incontri.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.deals

Utilizzato per fornire informazioni sulle offerte e le vendite online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.degree

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.delivery

Utilizzato da aziende che consegnano qualsiasi tipo di merce o servizio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.democrat

Utilizzato per informazioni sul partito democratico. Utilizzata anche da funzionari per cariche elette, funzionari eletti, appassionati di politica, consulenti e consiglieri.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.dental

Utilizzato da dentisti e fornitori di materiali dentali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.design

Utilizzato da chiese di qualsiasi dimensione o denominazione per comunicare con la parrocchia e pubblicare informazioni sugli eventi e le attività correlate alla chiesa.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.diamonds

Utilizzato da appassionati di diamanti e coloro che lavorano nel settore dei diamanti, tra cui venditori, rivenditori e merchandiser.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.diet

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .diet o trasferire domini .diet a Route 53. Continueremo a supportare i domini .diet che sono già registrati con Route 53.

Utilizzato da professionisti della salute e del fitness.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .diet a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.digital

Utilizzato per qualsiasi elemento digitale, ma ideale per aziende tecnologiche.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.direct

Utilizzato come estensione generale, ma ideale per le aziende che vendono prodotti direttamente ai clienti tramite un sito Web di e-commerce.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.directory

Utilizzato dal settore media.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.discount

Utilizzato per siti Web di sconto e aziende che riduce i prezzi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.dog

Utilizzato da amanti dei cani e da coloro che forniscono servizi e prodotti per cani.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.domains

Utilizzato per informazioni sui nomi di dominio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.education

Utilizzato per informazioni sulla formazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.email

Utilizzato per informazioni su e-mail di promozione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.energy

Utilizzato come estensione generale, ma ideale per coloro che lavorano nel campo dell'energia o della conservazione dell'energia.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.engineering

Utilizzato da studi tecnici e professionisti del settore.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.enterprises

Utilizzato per informazioni su aziende e società.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.equipment

Utilizzato per informazioni su apparecchiature, rivenditori di apparecchiature e negozi di noleggio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.estate

Utilizzato per informazioni sulle abitazioni e il settore abitativo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.events

Utilizzato per informazioni su eventi di ogni tipo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.exchange

Utilizzato per qualsiasi tipo di scambio: borsa, scambio di merci, o anche il semplice scambio di informazioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.expert

Utilizzato da coloro che hanno conoscenze specializzate in una serie di campi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.exposed

Utilizzato come estensione generica per un'ampia gamma di argomenti, tra cui la fotografia, i giornali e il giornalismo investigativo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.express

Utilizzato come estensione generale, ma ideale per chi desidera enfatizzare la rapida distribuzione di beni o servizi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fail

Utilizzato da chi ha commesso degli errori, ma ideale per la pubblicazione di errori e blooper divertenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fan

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.farm

Utilizzato da coloro che lavorano nel settore agricolo, ad esempio agricoltori e ingegneri agricoli.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.finance

Utilizzato dal settore finanziario.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.financial

Utilizzato dal settore finanziario.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fish

Utilizzato come estensione generale, ma ideale per siti Web correlati a pesci e pesca.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fitness

Utilizzato per promuovere fitness e servizi di fitness.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.flights

Utilizzato da agenti di viaggio, compagnie aeree e coloro che sono affiliati al settore dei viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.florist

Utilizzato da fiorai.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.flowers

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .flowers o trasferire domini .flowers a Route 53. Continueremo a supportare i domini .flowers che sono già registrati con Route 53.

Utilizzato per tutto ciò che è correlato ai fiori, ad esempio vendita di fiori online o informazioni sulla coltivazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .flowers a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fm

Per informazioni, consulta .fm (Stati Federati di Micronesia).

Return to index

.football

Utilizzato da coloro che sono coinvolti nello sport del calcio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.forsale

Utilizzato per la vendita di prodotti e servizi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.foundation

Utilizzato da organizzazioni no profit, organizzazioni di beneficenza e altri tipi di fondazioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fun

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fund

Utilizzato come estensione generale per tutto ciò che è correlato ai finanziamenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.furniture

Utilizzato dai produttori e rivenditori di mobili e chiunque è affiliato al settore dei mobili.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.futbol

Utilizzato per informazioni sul calcio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.fyi

Utilizzato come estensione generale, ma ideale per la condivisione di informazioni di ogni tipo. "FYI" è l'acronimo di "for your information", ovvero "per tua informazione".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gallery

Utilizzato da proprietari di gallerie d'arte.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.games

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gift

Utilizzato da aziende o organizzazioni che vendono regali o forniscono servizi correlati ai regali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gifts

Utilizzato da aziende o organizzazioni che vendono regali o forniscono servizi correlati ai regali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gives

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.glass

Utilizzato da coloro che lavorano nel settore vetro, come tagliatori e installatori di finestre.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.global

Utilizzato da aziende o gruppi con un mercato o una visione internazionale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, bielorusso, bosniaco, bulgaro, cinese semplificato, cinese tradizionale, danese, tedesco, hindi, ungherese, islandese, coreano, lettone, lituano, macedone, montenegrino, polacco, russo, serbo, spagnolo, svedese e ucraino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gmbh

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gold

Utilizzato come estensione generale, ma ideale per aziende che acquistano o vendono oro o prodotti correlati.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.golf

Utilizzato per siti Web dedicati al golf.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.graphics

Utilizzato da coloro che lavorano nel settore della grafica.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gratis

Utilizzato per i siti Web che offrono gratuitamente una serie di prodotti, come articoli promozionali, download o coupon. "Gratis" è un sinonimo di "gratuito".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.green

Utilizzato per siti Web dedicati a conservazione, ecologia, ambiente e stile di vita rispettoso dell'ambiente.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.gripe

Utilizzato per la condivisione di reclami e critiche.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.group

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.guide

Utilizzato come estensione generale, ma ideale per siti Web concentrati su destinazioni di viaggio e servizi e prodotti correlati.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.guitars

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .guitars o trasferire domini .guitars a Route 53. Continueremo a supportare i domini .guitars che sono già registrati con Route 53.

Utilizzato da appassionati di chitarra.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .guitars a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.guru

Utilizzato da coloro che desiderano condividere le proprie conoscenze su una serie di argomenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.haus

Utilizzato dal settore immobile ed edile. "Haus" è una parola tedesca che significa "casa".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.healthcare

Utilizzato per il settore sanitario.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.help

Utilizzato come estensione generale, ma ideale per siti Web che forniscono assistenza e informazioni online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.hiv

Utilizzato per siti Web dedicati alla lotta all'HIV.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.hockey

Utilizzato per siti Web dedicati all'hockey.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.holdings

Utilizzato da consulenti finanziari, agenti di borsa e coloro che lavorano con gli investimenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.holiday

Utilizzato da coloro che lavorano nel settore dei viaggi e da individui e aziende coinvolte nella pianificazione di feste e occasioni speciali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.host

Utilizzato da aziende che forniscono piattaforme e servizi di hosting Web.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, cinese semplificato, cinese tradizionale, greco, ebraico, coreano e tailandese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.hosting

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .hosting o trasferire domini .hosting a Route 53. Continueremo a supportare i domini .hosting che sono già registrati con Route 53.

Utilizzato per l'hosting di siti Web o da coloro che lavorano nel settore dell'hosting.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .hosting a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.house

Utilizzato da agenti immobiliari e acquirenti e venditori di case.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.im

Per informazioni, consulta .im (Isola di Man).

Return to index

.immo

Utilizzato dal settore immobiliare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.immobilien

Utilizzato per informazioni sul settore immobiliare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.industries

Utilizzato da qualsiasi azienda o impresa commerciale che desidera identificarsi come settore.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.info

Utilizzato per la diffusione di informazioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ink

Utilizzato da appassionati di tatuaggi o da qualsiasi settore correlato all'inchiostro, ad esempio il settore della stampa e della pubblicazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo e latino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.institute

Utilizzato da qualsiasi organizzazione o gruppo, soprattutto le organizzazioni di ricerca e di istruzione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.insure

Utilizzato da compagnie assicurative e intermediari assicurativi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.international

Utilizzato da aziende che hanno catene internazionali, individui che viaggiano a livello internazionale, oppure organizzazioni di beneficenza con un'influenza internazionale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.investments

Utilizzato come estensione generale, ma ideale per la promozione di opportunità di investimento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.io

Per informazioni, consulta .io (Territorio britannico dell'Oceano Indiano).

Return to index

.irish

Utilizzato per promuovere la cultura e le organizzazioni irlandesi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, cinese semplificato, cinese tradizionale, francese, tedesco, greco, ebraico, giapponese, coreano, spagnolo, tamil e tailandese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.jewelry

Utilizzato da acquirenti e venditori di gioielli.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.juegos

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .juegos o trasferire domini .juegos a Route 53. Continueremo a supportare i domini .juegos che sono già registrati con Route 53.

Utilizzato per siti Web di giochi di ogni tipo. "Juegos" è una parola spagnola che significa "giochi".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .juegos a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.kaufen

Utilizzato per informazioni sull'e-commerce.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.kim

Utilizzato dagli utenti il cui nome o cognome è Kim.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.kitchen

Utilizzato da rivenditori di cucine, cuochi, blogger di cibo e da coloro che lavorano all'interno dell'industria alimentare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.kiwi

Utilizzato per le aziende e le persone che desiderano supportare la cultura kiwi neozelandese. Viene inoltre utilizzato come piattaforma per organizzazioni caritative nella ricostruzione di Christchurch, danneggiata da terremoti nel 2010 e 2011.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per il maori.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.land

Utilizzato da agricoltori, agenti immobiliari, sviluppatori commerciali, e chiunque sia interessato nelle proprietà.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.legge

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.lease

Utilizzato da agenti immobiliari, proprietari e affittuari.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.legal

Utilizzato da membri di professioni giuridiche.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.lgbt

Utilizzato dalle comunità di lesbiche, gay, bisessuali e transessuali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.life

Utilizzato come estensione generale, e idoneo per un'ampia gamma di aziende, gruppi e individui.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.lighting

Utilizzato da fotografi, designer, architetti, ingegneri e altri utenti con un interesse nell'illuminazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.limited

Utilizzato come estensione generale, e idoneo per un'ampia gamma di aziende, gruppi e individui.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.limo

Utilizzato da autisti, aziende di limousine e agenzie di autonoleggio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.link

Utilizzato per informazioni sulla creazione di collegamenti online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Uniregistry è il registro per i domini .LINK. A causa della politica di Uniregistry, il livello di registro WHOIS mostra "REDACTED FOR PRIVACY" ("CENSURATO PER LA PRIVACY"). La rimozione della nostra funzione di protezione della privacy influirà solo sulle informazioni visualizzate a livello di registrar Amazon Registrar WHOIS.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.live

Utilizzato come estensione generale, e idoneo per un'ampia gamma di aziende, gruppi e individui.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.llc

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.loan

Utilizzato da mutuanti, mutuatari e professionisti del credito.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per danese, tedesco, norvegese e svedese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.loans

Utilizzato da mutuanti, mutuatari e professionisti del credito.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.lol

Utilizzato per siti Web di umorismo e commedia. "LOL" è l'acronimo di "laugh out loud", ovvero "ridere a voce alta".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico, francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ltd

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.maison

Utilizzato dal settore immobiliare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.management

Utilizzato per informazioni sul mondo del business e la gestione d'impresa.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.marketing

Utilizzato dal settore del marketing per un'ampia gamma di scopi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.mba

Utilizzato per i siti Web che forniscono informazioni sul master in amministrazione aziendale (MBA).

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.media

Utilizzato dal settore media e intrattenimento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.memorial

Utilizzato da organizzazioni commemorative dedicate a onorare eventi e persone.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.mobi

Utilizzato da aziende e persone che desiderano rendere i propri siti Web accessibili da cellulare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.moda

Utilizzato per informazioni sulla moda.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.money

Utilizzato per i siti Web che si concentrano sulle attività in materia di denaro.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.mortgage

Utilizzato dal settore dei mutui.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.movie

Utilizzato per i siti Web che forniscono informazioni sui film e regia. Adatto sia per i professionisti che per i fan.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.name

Utilizzato da chiunque desideri creare una presenza Web personalizzata.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Verisign, il registro per .name TLDs, consente di registrare sia domini di secondo livello (name .name) che domini di terzo livello (firstname). cognome (.name). Route 53 supporta solo domini di secondo livello, sia per la registrazione di domini che per trasferire domini esistenti a Route 53.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.net

Utilizzato per tutti i tipi di siti Web. L'estensione.net è un'abbreviazione di network, ovvero rete.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.network

Utilizzato da coloro che lavorano nel settore delle reti o da chi desidera creare connessioni tramite reti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.news

Utilizzato per distribuire qualsiasi notizia come eventi correnti o informazioni relative a giornalismo e comunicazione.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ninja

Utilizzato da individui e aziende che vogliono associarsi alle capacità di un ninja.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.onl

L'estensione.onl è l'abbreviazione di "online", ed è anche l'abbreviazione spagnola per le organizzazioni no profit.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, bielorusso, bosniaco, bulgaro, cinese (semplificato e tradizionale), danese, tedesco, hindi, ungherese, islandese, coreano, lettone, lituano, macedone, polacco, russo, serbo e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.online

L'estensione.onl è l'abbreviazione di "online", ed è anche l'abbreviazione spagnola per le organizzazioni no profit.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.org

Utilizzato da tutti i tipi di organizzazioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.partners

Utilizzato da studi legali, investitori e un'ampia gamma di aziende. Utilizzato anche per siti Web social che creano relazioni.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.parts

Utilizzato come estensione generale, ma ideale per produttori, venditori e acquirenti di parti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.photo

Utilizzato da fotografi e da chiunque sia interessato alle foto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza

- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.photography

Utilizzato da fotografi e da chiunque sia interessato alle foto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.photos

Utilizzato da fotografi e da chiunque sia interessato alle foto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pics

Utilizzato da fotografi e da chiunque sia interessato alle foto.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pictures

Utilizzato da chiunque sia interessato alla fotografia, all'arte e al multimediale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pink

Utilizzato da chi ama il rosa o da coloro che desiderano associare il colore rosa al proprio business o marchio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pizza

Utilizzato da pizzerie e amanti della pizza.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.place

Utilizzato come estensione generale, ma ideale per i settori della casa e dei viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.plumbing

Utilizzato da coloro che lavorano nel settore idraulico.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.plus

Utilizzato come estensione generale, ma ideale per il vestiario di taglie forti, il software aggiuntivo o qualsiasi prodotto che offre caratteristiche o dimensioni "extra".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.poker

Utilizzato da giocatori di poker e siti Web di gioco.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.porn

Utilizzato per siti Web per soli adulti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.press

Utilizzato per siti Web per soli adulti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pro

Utilizzato da professionisti qualificati e accreditati e da organizzazioni professionali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.productions

Utilizzato da studi e case di produzione che realizzano annunci pubblicitari, radiofonici e video musicali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.properties

Utilizzato per informazioni su qualsiasi tipo di proprietà, tra cui immobili o proprietà intellettuale. Utilizzato anche da coloro che possiedono abitazioni, edifici o terreni da vendere, noleggiare o affittare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.property

Utilizzato per informazioni su qualsiasi tipo di proprietà, tra cui immobili o proprietà intellettuale. Utilizzato anche da coloro che possiedono abitazioni, edifici o terreni da vendere, noleggiare o affittare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .property a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.pub

Utilizzato da coloro che lavorano nel campo della pubblicazione, pubblicità o della birra.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.qpon

Utilizzato per coupon e codici promozionali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per lo spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.recipes

Utilizzato da coloro che hanno ricette da condividere.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.red

Utilizzato da chi ama il rosso o da coloro che desiderano associare il colore rosso al proprio business o marchio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.reise

Utilizzato per siti Web correlati a viaggi. "Reise" è una parola tedesca che significa "nascita", "sorgere", o "partire".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.reisen

Utilizzato per siti Web correlati a viaggi. "Reisen" è una parola tedesca che significa "viaggiare".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.rentals

Utilizzato per tutti i tipi di noleggio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.repair

Utilizzato da servizi di riparazione o da coloro che desiderano insegnare come riparare tutti i tipi di articoli.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.report

Utilizzato come estensione generale, ma ideale per informazioni sui report aziendali, pubblicazioni di community, report su libri o comunicazioni di notizie.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.republican

Utilizzato per informazioni sul partito repubblicano. Utilizzata anche da funzionari per cariche elette, funzionari eletti, appassionati di politica, consulenti e consiglieri.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.restaurant

Utilizzato dal settore dei ristoranti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.reviews

Utilizzato da chi desidera offrire le proprie opinioni e leggere i commenti degli altri utenti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.rip

Utilizzato per siti Web dedicato a morte e memorial. "RIP" è l'acronimo di "riposa in pace".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.rocks

Utilizzato come estensione generale, ma ideale per chiunque abbia a che fare con il rock o con le pietre: musicisti, geologi, gioiellieri, scalatori e molto altro.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.run

Utilizzato come estensione generale, ma ideale per il settore del fitness e dello sport.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.sale

Utilizzato dai siti Web di e-commerce.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.sarl

Utilizzato da società a responsabilità limitata generalmente con sede in Francia. "SARL" è l'acronimo di Société à Responsabilité Limité.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.school

Utilizzato per informazioni sulla formazione, gli istituti scolastici e le attività correlate alla scuola.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.schule

Utilizzato per informazioni sulla formazione, gli istituti scolastici e le attività correlate alla scuola, il tutto correlato al tedesco. "Schule" è una parola tedesca che significa "scuola".

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.services

Utilizzato per siti Web concentrati su servizi di qualsiasi tipo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.sex

Utilizzato per contenuti per soli adulti.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.sexy

Utilizzato per contenuti di natura sessuale. Utilizzato anche per descrivere i brand, i prodotti, le informazioni e i siti Web più popolari ed entusiasmanti.

Return to index

> **Important**
>
> Non puoi più utilizzare Route 53 per registrare nuovi domini .sexy o trasferire domini .sexy a Route 53. Continueremo a supportare i domini .sexy già registrati con Route 53.

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non puoi più trasferire domini .sexy a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.shiksha

Utilizzato da istituzioni educative. "Shiksha" è un termine Indiano per scuola.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.shoes

Utilizzato da rivenditori, designer, produttori o fashion blogger di calzature.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.acquisti

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.show

Utilizzato come estensione generale, ma ideale per il settore dell'intrattenimento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.singles

Utilizzato da servizi di appuntamento, resort e altre aziende che si rivolgono a coloro che desiderano connettersi con altre persone.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.site

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ski

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.soccer

Utilizzato per siti Web dedicati al calcio.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.social

Utilizzato per informazioni sui social network, i forum e le conversazioni online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.solar

Utilizzato per informazioni sul sistema solare o l'energia solare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.solutions

Utilizzato da consulenti, do-it-yourself servizi e consulenti di ogni tipo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.software

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.space

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.store

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.stream

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.studio

Utilizzato come estensione generale, ma ideale per coloro che lavorano nel campo degli immobili, dell'arte o dell'intrattenimento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.style

Utilizzato come estensione generale, ma ideali per siti Web dedicati alle ultime tendenze, soprattutto i trend di moda, design, architettura e arte.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.sucks

Utilizzato come estensione generale, ma la soluzione ideale per chi desidera condividere esperienze negative o avvisare altri utenti su truffe, frodi o prodotti danneggiati.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.supplies

Utilizzato da aziende che vendono merci online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.supply

Utilizzato da aziende che vendono merci online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.support

Utilizzato da aziende, gruppi o associazioni di beneficenza che offrono qualsiasi tipo di supporto, tra cui assistenza clienti, assistenza prodotto o supporto emotivo, finanziario o spirituale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.surgery

Utilizzato per informazioni su chirurgia, medicina, e assistenza sanitaria.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.systems

Utilizzato principalmente per il settore tecnologico e da coloro che offrono servizi tecnologici.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tattoo

Utilizzato da appassionati di tatuaggi e dal settore dei tatuaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cirillico (principalmente russo), francese, tedesco, italiano, portoghese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tax

Utilizzato per informazioni sulle imposte, preparazione delle dichiarazioni fiscali e diritto fiscale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.taxi

Utilizzato da aziende di taxi, autisti e navette.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.team

Utilizzato da qualsiasi azienda o organizzazione che desidera identificarsi come team.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tech

Utilizzato da appassionati di tecnologia e da aziende, servizi e produttori tecnologici.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.technology

Utilizzato da appassionati di tecnologia e da aziende, servizi e produttori tecnologici.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tennis

Utilizzato per informazioni relative al tennis.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.theater

Utilizzato per siti Web dedicati a teatri, rappresentazioni e musical.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tienda

Utilizzato da aziende di vendita al dettaglio che vogliono entrare in contatto con i consumatori di lingua spagnola.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tips

Utilizzato da coloro che desiderano condividere le proprie conoscenze e consigli su qualsiasi argomento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tires

Utilizzato da produttori, distributori o acquirenti di pneumatici.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.today

Utilizzato per informazioni sugli eventi attuali, le notizie, il meteo, l'intrattenimento e molto altro.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tools

Utilizzato per informazioni su qualsiasi tipo di strumento.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tours

Utilizzato come estensione generale, ma ideale per le società del settore viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.town

Utilizzato per promuovere le tradizioni, la cultura e la comunità di una città.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.toys

Utilizzato dal settore dei giocattoli.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.trade

Utilizzato come estensione generale, ma ideale per siti Web di commercio o servizi commerciali.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per danese, tedesco, norvegese e svedese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.training

Utilizzato da trainer, coach ed educatori.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.tv

Utilizzato per informazioni su televisione e media.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Nessuna.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.university

Utilizzato da università e altre organizzazioni educative.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.uno

Utilizzato per informazioni sulle comunità ispaniche, portoghesi e italiane.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per lo spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.vacations

Utilizzato dal settore di viaggi e turismo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.vegas

Utilizzato per promuovere la città di Las Vegas e lo stile di vita di Las Vegas.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.ventures

Utilizzato da imprenditori, start-up, venture capitalist, banche di investimento e finanzieri.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza

- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.vg

Per informazioni, consulta .vg (Isole Vergini britanniche).

Return to index

.viajes

Utilizzato da agenzie di viaggio, operatori turistici, blog di viaggio, aziende turistiche, servizi di noleggio, blogger di viaggio e rivenditori di viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.video

Utilizzato dal settore media e video.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco, latino e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.villas

Utilizzato da agenti immobiliari e proprietari di immobili che hanno ville da vendere o affittare.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.vision

Utilizzato come estensione generale, ma ideale per gli specialisti della vista, come oculisti e simili.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.voto

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.voyage

Utilizzato da agenzie di viaggio, operatori turistici, blog di viaggio, aziende turistiche, servizi di noleggio, blogger di viaggio e rivenditori di viaggi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.watch

Utilizzato per informazioni su siti Web, web TVs, video o orologi in streaming.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.website

Utilizzato per informazioni sullo sviluppo, la promozione, i miglioramenti e le esperienze sui siti Web.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, cinese semplificato, cinese tradizionale, greco, ebraico, giapponese, coreano e tailandese.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.wedding

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Nessuna.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per cinese, francese, tedesco e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.wiki

Utilizzato per informazioni sulla documentazione online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo e latino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.wine

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy

Supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.lavoro

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.works

Utilizzato da aziende, organizzazioni e singoli per informazioni sul lavoro, le mansioni e i servizi di collocamento. Questa estensione può essere utilizzata come un'alternativa alle estensioni .com, .net o .org.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.world

Utilizzato da chiunque desideri fornire informazioni su argomenti a livello globale.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.wtf

Utilizzato da chiunque desideri identificarsi con il popolare (ma blasfemo) acronimo "WTF."

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.xyz

Utilizzato come estensione generale per qualsiasi scopo.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Il record per i domini .xyz, Generation XYZ, considera alcuni nomi di dominio come nomi premium. Non è possibile eseguire la registrazione di domini premium .xyz o trasferirli a Route 53. Per ulteriori informazioni, consulta il sito Web di Generation XYZ.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.zone

Utilizzato per informazioni su qualsiasi tipo di zona, tra cui aree geografiche, zone climatiche e zone sportive.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per francese e spagnolo.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

Domini di primo livello geografici

Le seguenti estensioni di dominio sono raggruppate per area geografica e includono estensioni ufficiali specifiche del paese, note come domini di primo livello con codice nazionale (cc). TLDs Alcuni esempi sono .be (Belgio), .in (India) e .mx (Messico). Le regole per la registrazione di cc variano in base al Paese. TLDs Alcuni paesi non prevedono restrizioni, il che significa che chiunque al mondo può registrare tali domini, mentre altri prevedono restrizioni, ad esempio la residenza. L'elenco di ogni ccTLD indica eventuali restrizioni.

> **Important**
>
> Durante il trasferimento di qualsiasi cc TLDs a Route 53, ad eccezione di .cc e .tv, gli aggiornamenti al contatto del proprietario vengono ignorati e vengono utilizzati i dati di contatto del proprietario presenti nel registro. Una volta completato il trasferimento, puoi aggiornare le informazioni di contatto del proprietario. Per ulteriori informazioni, consulta Aggiornamento delle informazioni di contatto e di proprietà per un dominio.

Return to index

Africa

.ac (Isola di Ascensione), .co.za (Sudafrica), .sh (Saint Helena)

Americhe

.ca (Canada), .cl (Cile), .co (Colombia), .com.ar (Argentina), .com.br (Brasile), com.mx (Messico), .mx (Messico), .us (Stati Uniti), .vc (Saint Vincent e Grenadine), .vg (Isole Vergini britanniche)

Asia/Oceania

.au (Australia), .cc (Isole Cocos), .co.nz (Nuova Zelanda), .com.au (Australia), .com.sg (Repubblica di Singapore), .fm (Stati Federati di Micronesia), .in (India), .jp (Japan), .io (Territorio britannico dell'Oceano Indiano), .net.au (Australia), .net.nz (Nuova Zelanda), .org.nz (Nuova Zelanda), .pw (Palau), .qa (Qatar), .ru (Federazione russa), .sg (Repubblica di Singapore)

Europa

.be (Belgio), .berlin (città di Berlino in Germania), .ch (Svizzera), .co.uk (Regno Unito), .cz (Repubblica Ceca), .de (Germania), .es (Spagna) , .eu (Unione europea), .fi (Finlandia), .fr (Francia), .gg (Guernsey), .im (Isola di Man), .it (Italia), .me (Montenegro), .me.uk (Regno Unito), .nl (Paesi Bassi), .org.uk (Regno Unito), .ruhr (regione della Ruhr, parte occidentale della Germania), .se (Sweden), .uk (United Kingdom), .wien (città di Vienna in Austria)

Africa

Puoi utilizzare i seguenti domini di primo livello (TLDs) per l'Africa per registrare domini con Amazon Route 53.

, ,

Return to index

.ac (Isola di Ascensione)

Return to index

Utilizzato anche come TLD generico, popolare per il mondo accademico.

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 80 giorni dopo la scadenza

.co.za (Sudafrica)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Solo i domini di secondo livello sono disponibili per l'estensione .za. Route 53 supporta il dominio di secondo livello .co.za.

Aperto al pubblico, con alcune restrizioni:

- La registrazione è aperta a persone giuridiche identificabili (individui e persone giuridiche).
- Il nome di dominio deve superare un controllo di zona durante la procedura di registrazione.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Per prevenire trasferimenti non autorizzati, limita l'accesso all'indirizzo e-mail del registrante e alla Route 53, APIs che potrebbero consentire il cambio di proprietà, ad esempio,. UpdateDomainContact Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per i domini di Route 53 in Service Authorization Reference e Autorizzazioni di esempio per il proprietario di un record di dominio.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

No

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a un giorno prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 1 giorno prima della scadenza
- Il ripristino con il record è possibile: tra 1 e 9 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 9 giorni dopo la scadenza

.sh (Saint Helena)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 80 giorni dopo la scadenza

Americhe

Puoi utilizzare i seguenti domini di primo livello (TLDs) per le Americhe per registrare domini con Amazon Route 53.

, , , , , , , , ,

Return to index

.ca (Canada)

Return to index

Le varianti, con (à) o senza (a) un accento, di un nome di dominio sono automaticamente riservate al registrante e diventano parte di un pacchetto amministrativo. Per attivare un dominio in un pacchetto, il registrante deve effettuare una richiesta di registrazione per il dominio. Tutti i domini inclusi in un pacchetto devono essere registrati dallo stesso registrante e presso lo stesso registrar. Il registrante dovrà inoltre inviare una richiesta di trasferimento per tutti i domini inclusi in un pacchetto per completare il trasferimento.

E-mail di conferma dal record del TLD

Quando record un dominio .ca, riceverai un'e-mail con un link alla procedura di accettazione del contratto per il registrant. È necessario completare la procedura entro 7 giorni o il dominio non verrà registrato.

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- La registrazione è aperta a individui o organizzazioni correlati al Canada, come descritto dai requisiti di presenza canadesi per i registrant.
- Contatto del registrant: è necessario fornire il nome legale completo ed esatto del proprietario del dominio.
- Contatti amministrativi e tecnici: è necessario specificare Person (Persona) come tipo di contatto e fornire informazioni di contatto per gli individui residenti in Canada.
- È necessario selezionare uno dei seguenti tipi legali durante la procedura di registrazione:
  - ABO: popoli aborigeni (individui o gruppi) indigeni del Canada
  - ASS: Canadian unincorporated association
  - CCO: Canadian corporation, o provincia o territorio canadese
  - CCT: cittadino canadese
  - EDU: istituto educativo canadese
  - GOV: governo o enti governativi in Canada
  - HOP: ospedale canadese
  - INB: Indian Band riconosciuto dall'Indian Act of Canada
  - LAM: biblioteca, archivio o museo canadese
  - LGR: Rappresentante legale di un cittadino canadese o residente permanente

- UOMO: Her/His Majesty the Queen/King
- OMK: marchio ufficiale registrato in Canada
- PLT: partito politico canadese
- PRT: partnership registrata in Canada
- RES: residente permanente del Canada
- TDM: marchio registrato in Canada (da un tipo di proprietario non canadese)
- TRD: sindacato canadese
- TRS: trust stabilito in Canada

Protezione della privacy

- Persona: per tutti i contatti, il nome, l'indirizzo, il numero di telefono, il numero di fax e l'indirizzo e-mail del contatto sono nascosti, poiché CIRA applica automaticamente la protezione della privacy a una persona. L'opzione di protezione della privacy verrà applicata solo al registrar Whois.
- Azienda, associazione o ente pubblico: non supportata a livello di registro.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: data variabile. Contatta il supporto AWS.

Eliminazione della registrazione di dominio

Il record per domini .ca non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.cl (Cile)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .cl o trasferire domini .cl a Route 53. Continueremo a supportare i domini .cl che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Due anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .cl a Route 53.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: contatta AWS Support.
- Il rinnovo tardivo con Route 53 è possibile: contatta AWS Support.

- Il dominio viene eliminato da Route 53: contatta AWS Support.
- Il ripristino con il record è possibile: contatta AWS Support.
- Il dominio viene eliminato dal record: contatta AWS Support.

.co (Colombia)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a cinque anni.

Restrizioni

Il record dei domini .co, Go.co, considera alcuni nomi di dominio come nomi di dominio premium. Non è possibile eseguire la registrazione di domini premium .co o trasferirli a Route 53. Per ulteriori informazioni, consulta il sito Web Go.co.

Protezione della privacy (si applica a: persona)

Tutte le informazioni sono nascoste.

Se il tipo di contatto non è una persona, il nome dell'azienda e il paese vengono visualizzati da WHOIS.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 45 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 50 giorni dopo la scadenza

.com.ar (Argentina)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .com.ar o trasferire domini .com.ar a Route 53. Continueremo a supportare i domini .com.ar che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Un anno.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Per prevenire trasferimenti non autorizzati, limita l'accesso all'indirizzo e-mail del registrante e alla Route 53, APIs che potrebbero consentire il cambio di proprietà, ad esempio,. UpdateDomainContact Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per i domini di Route 53 in Service Authorization Reference e Autorizzazioni di esempio per il proprietario di un record di dominio.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .com.ar a Route 53.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: contatta AWS Support.
- Il rinnovo tardivo con Route 53 è possibile: contatta AWS Support.

- Il dominio viene eliminato da Route 53: contatta AWS Support.
- Il ripristino con il record è possibile: contatta AWS Support.
- Il dominio viene eliminato dal record: contatta AWS Support.

.com.br (Brasile)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .com.br o trasferire domini .com.br a Route 53. Continueremo a supportare i domini .com.br che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Un anno.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .com.br a Route 53.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 30 giorni prima della scadenza e la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 119 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 119 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 119 giorni dopo la scadenza

com.mx (Messico)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.mx (Messico)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.us (Stati Uniti)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Il record per domini .us non consente l'utilizzo di nomi di dominio che contengono le sette parole identificate nella "Appendice del parere della Corte" della Federal Communications Commission v. Pacifica Foundation No. 77-528

Aperto al pubblico, con una restrizione:

- L'estensione .us è per i siti Web o le attività che sono situate negli Stati Uniti.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 65 giorni dopo la scadenza

.vc (Saint Vincent e Grenadine)

Utilizzato anche come TLD generico, spesso da coloro coinvolti nel finanziamento di venture capitale, varsity college e così via.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 80 giorni dopo la scadenza

.vg (Isole Vergini britanniche)

Utilizzato anche come TLD generico, spesso da organizzazioni coinvolte nei videogiochi.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a 44 giorni dopo la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: Sì
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 74 giorni dopo la scadenza
- Il dominio viene reso pubblicamente disponibile di nuovo: 80 giorni dopo la scadenza

Asia/Oceania

Puoi utilizzare i seguenti domini di primo livello (TLDs) per Asia e Oceania per registrare domini con Amazon Route 53.

, , , , , , , , , , , , , , ,

Return to index

.au (Australia)

Return to index

E-mail di conferma dal record del TLD

Il nostro registrar associato, Gandi, rivende i domini.au tramite. DomainDirectors Quando trasferisci un nome di dominio su Route 53, DomainDirectors invia un'e-mail al referente del registrante del dominio per verificare le informazioni di contatto o autorizzare le richieste di trasferimento.

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- I domini .au sono aperti a persone giuridiche, associazioni commerciali, partnership o società individuali registrate in Australia; a imprese straniere con licenza di commerciare in Australia e a proprietari o candidati per un marchio registrato australiano. Le persone fisiche non possono registrare domini .au. Il contatto del registrant deve essere una società.
- Il tuo nome di dominio deve essere identico al tuo nome (come registrato con l'autorità australiana pertinente) o al tuo marchio (o all'abbreviazione o all'acronimo).
- Il nome di dominio deve indicare la tua attività. Ad esempio, deve indicare un prodotto che vendi o un servizio che fornisci.
- Durante il processo di registrazione, è necessario indicare le informazioni riportate di seguito.
  - Il tuo tipo di registrazione: ABN (Australian Business Number), ACN (Australian Company Number) o TM (Trademark) se il nome di dominio corrisponde al tuo marchio.
  - Il tuo numero ID, che può essere un numero di carta Medicare, un numero fiscale (TFN), un numero di patente o un Australian Business Number (ABN).
  - Il tuo stato o provincia.
- Informazioni di contatto errate o non corrispondenti, tra cui nome, ABN o numero di marchio (TM), comporteranno errori di registrazione, commercio e rinnovi. Potrebbe essere necessaria una modifica della proprietà per correggere le informazioni per i domini esistenti.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'API. RetrieveDomainAuthCode (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì. Oltre alla console Route 53, puoi anche ottenere il codice di trasferimento dal registro.au.

DNSSEC

Supportato per la registrazione del dominio. Quando si imposta la chiave, è necessario scegliere l'algoritmo di sicurezza DNS 2 (DH). Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 60 giorni prima della scadenza e la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 29 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 30 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il registro dei domini .au non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

Modifica della proprietà

Modifica il proprietario utilizzando la console Route 53. Per informazioni, consulta Aggiornamento delle informazioni di contatto per un dominio. Quindi completa il seguente processo per completare la modifica di proprietà:

1. Sia i vecchi che i nuovi iscritti devono fare clic sul collegamento ricevuto in un'e-mail da transfers@1api.net agli indirizzi e-mail elencati. Se questo non viene completato entro 14 giorni, dovrai riavviare il processo.

2. Una volta confermate le risposte, la modifica del proprietario nel registro verrà elaborata in breve tempo senza ulteriori conferme.

.cc (Isole Cocos)

Return to index

Utilizzato anche come TLD generico, spesso da organizzazioni con "cc" nel nome, come società di consulenza, provider di soluzioni di cloud computing, o club di ciclismo. L'estensione è un'alternativa popolare a ".com".

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

- Nascosto: indirizzo, numero di telefono, numero di fax e indirizzo e-mail
- Non nascosto: nome di contatto e nome dell'organizzazione

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 65 giorni dopo la scadenza

.co.nz (Nuova Zelanda)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Puoi registrare i seguenti domini di secondo livello con Route 53: .co.nz, .net.nz e .org.nz. Non è possibile registrare domini .nz (di primo livello) con Route 53 o trasferire domini .nz a Route 53.

Aperto al pubblico, con alcune restrizioni:

- Gli individui devono avere almeno 18 anni.
- Le organizzazioni devono essere registrate.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 44 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 44 e 134 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 134 giorni dopo la scadenza

.com.au (Australia)

Return to index

E-mail di conferma dal record del TLD

Il nostro registrar associato, Gandi, rivende i domini.com.au tramite. DomainDirectors Quando trasferisci un nome di dominio su Route 53, DomainDirectors invia un'e-mail al referente del registrante del dominio per verificare le informazioni di contatto o autorizzare le richieste di trasferimento.

Periodo di locazione della registrazione e rinnovo

Da uno a cinque anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- I domini .com.au e .net.au sono aperti a partnership o società individuali registrate in Australia; a imprese straniere con licenza di commerciare in Australia e a proprietari o candidati per un marchio registrato australiano. Gli individui non possono registrare domini .com.au/.net.au. Il contatto del registrant deve essere una società.
- Il tuo nome di dominio deve essere identico al tuo nome (come registrato con l'autorità australiana pertinente) o al tuo marchio (o all'abbreviazione o all'acronimo per il tuo marchio).
- Il nome di dominio deve indicare la tua attività. Ad esempio, deve indicare un prodotto che vendi o un servizio che fornisci.
- Durante il processo di registrazione, è necessario fornire le informazioni riportate di seguito.

- Il tuo tipo di registrazione: ABN (Australian Business Number), ACN (Australian Company Number) o TM (Trademark) se il nome di dominio corrisponde al tuo marchio.
- Il tuo numero ID, che può essere ABN (Australian Business Number), ACN (Australian Company Number) o il tuo marchio commerciale (TM) se il nome dominio corrisponde al tuo marchio commerciale.
- Il tuo stato o provincia.

- Informazioni di contatto errate o non corrispondenti, tra cui nome, ABN o numero di marchio (TM), comporteranno errori di registrazione, commercio e rinnovi. Potrebbe essere necessaria una modifica della proprietà per correggere le informazioni per i domini esistenti.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'API. RetrieveDomainAuthCode (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Quando si imposta la chiave, è necessario scegliere l'algoritmo di sicurezza DNS 2 (DH). Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 60 giorni prima della scadenza e la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 29 giorni dopo la scadenza
- Il ripristino con il record è possibile: no

- Il dominio viene eliminato dal record: 30 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .com.au non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

Modifica della proprietà

Modifica il proprietario, a livello di codice o utilizzando la console Route 53. Per informazioni, consulta Aggiornamento delle informazioni di contatto per un dominio. Quindi completa il seguente processo per completare la modifica di proprietà:

1. Sia i vecchi che i nuovi iscritti devono fare clic sul collegamento ricevuto in un'e-mail da transfers@1api.net agli indirizzi e-mail indicati. Se questo non viene completato entro 14 giorni, dovrai riavviare il processo.

2. Una volta confermate le risposte, la modifica del proprietario nel registro verrà elaborata in breve tempo senza ulteriori conferme.

.com.sg (Repubblica di Singapore)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .com.sg o trasferire domini .com.sg a Route 53. Continueremo a supportare i domini .com.sg che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Uno o due anni.

Eliminazione della registrazione di dominio

Il record per domini .com.sg non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .com.sg a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 60 giorni dopo la scadenza

.fm (Stati Federati di Micronesia)

Utilizzato anche come TLD generico, spesso da organizzazioni coinvolte in media e trasmissioni online.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 44 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 44 e 79 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 84 giorni dopo la scadenza

.in (India)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 65 giorni dopo la scadenza

.jp (Japan)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, con una restrizione:

- Solo privati o aziende in Giappone possono registrare un nome di dominio .jp.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per il giapponese.

Codice di autorizzazione richiesto per i trasferimenti

Sì.

Il registro.jp gestisce il codice di autorizzazione con a time-to-live e potrebbe scadere. Puoi aggiornare il codice di autenticazione rimuovendo lo stato transfer lock (clientTransferProhibited) dal tuo dominio, se presente. Se il dominio non ha alcun blocco di trasferimento, puoi aggiornare il codice di autenticazione attivandolo prima e poi disattivandolo.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 30 e 7 giorni prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 6 giorni prima della scadenza
- Il ripristino con il record è possibile: contatta AWS Support.
- Il dominio viene eliminato dal record: contatta AWS Support.

> **Note**
>
> Al momento non è possibile registrare domini non-general-purpose JP come .co.jp e.or.jp.

.io (Territorio britannico dell'Oceano Indiano)

Utilizzato anche come TLD generico, spesso da organizzazioni informatiche quali servizi online, giochi basati su browser e startup.

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Tutte le informazioni sono nascoste, tranne stato/provincia e paese.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

Il record per domini .io, inoltre, usa il codice di autorizzazione come una password a uso singolo per alcune operazioni, ad esempio l'abilitazione o la disabilitazione della protezione della privacy. Se desideri eseguire più di un'operazione che richiede una password, devi generare un altro codice di autorizzazione per ciascuna operazione.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal registro: 90 giorni dopo la scadenza

.net.au (Australia)

Return to index

E-mail di conferma dal record del TLD

Il nostro registrar associato, Gandi, rivende i domini.net.au tramite. DomainDirectors Quando trasferisci un nome di dominio su Route 53, DomainDirectors invia un'e-mail al referente del registrante del dominio per verificare le informazioni di contatto o autorizzare le richieste di trasferimento.

Periodo di locazione della registrazione e rinnovo

Da uno a cinque anni.

Restrizioni

Sono disponibili solo domini di secondo livello. Route 53 supporta i domini di secondo livello .com.au e net.au.

Aperto al pubblico, con alcune restrizioni:

- I domini .com.au e .net.au sono aperti a persone giuridiche, associazioni commerciali, partnership o società individuali registrate in Australia; a imprese straniere con licenza di commerciare in Australia e a proprietari o candidati per un marchio registrato australiano.
- Il tuo nome di dominio deve essere identico al tuo nome (come registrato con l'autorità australiana pertinente) o al tuo marchio (o all'abbreviazione o all'acronimo).
- Il nome di dominio deve indicare la tua attività. Ad esempio, deve indicare un prodotto che vendi o un servizio che fornisci.
- Durante il processo di registrazione, è necessario indicare le informazioni riportate di seguito.
  - Il tuo tipo di registrazione: ABN (Australian Business Number), ACN (Australian Company Number) o TM (Trademark) se il nome di dominio corrisponde al tuo marchio.
  - Il tuo numero ID, che può essere ABN (Australian Business Number), ACN (Australian Company Number) o il tuo marchio commerciale (TM) se il nome dominio corrisponde al tuo marchio commerciale.
  - Il tuo stato o provincia.
- Informazioni di contatto errate o non corrispondenti, tra cui nome, ABN o numero di marchio (TM), comporteranno errori di registrazione, commercio e rinnovi. Potrebbe essere necessaria una modifica della proprietà per correggere le informazioni per i domini esistenti.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'API. RetrieveDomainAuthCode (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Quando si imposta la chiave, è necessario scegliere l'algoritmo di sicurezza DNS 2 (DH). Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 60 giorni prima della scadenza e la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 29 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 30 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .net.au non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

Modifica della proprietà

Modifica il proprietario, a livello di codice o utilizzando la console Route 53. Per informazioni, consulta Aggiornamento delle informazioni di contatto per un dominio. Quindi completa il seguente processo per completare la modifica di proprietà:

1. Sia i vecchi che i nuovi iscritti devono fare clic sul collegamento ricevuto in un'e-mail da transfers@1api.net agli indirizzi e-mail indicati. Se questo non viene completato entro 14 giorni, dovrai riavviare il processo.

2. Una volta confermate le risposte, la modifica del proprietario nel registro verrà elaborata in breve tempo senza ulteriori conferme.

.net.nz (Nuova Zelanda)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Puoi registrare i seguenti domini di secondo livello con Route 53: .co.nz, .net.nz e .org.nz. Non è possibile registrare domini .nz (di primo livello) con Route 53 o trasferire domini .nz a Route 53.

Aperto al pubblico, con alcune restrizioni:

- Gli individui devono avere almeno 18 anni.
- Le organizzazioni devono essere registrate.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 44 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 44 e 134 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 134 giorni dopo la scadenza

.org.nz (Nuova Zelanda)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Puoi registrare i seguenti domini di secondo livello con Route 53: .co.nz, .net.nz e .org.nz. Non è possibile registrare domini .nz (di primo livello) con Route 53 o trasferire domini .nz a Route 53.

Aperto al pubblico, con alcune restrizioni:

- Gli individui devono avere almeno 18 anni.
- Le organizzazioni devono essere registrate.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 44 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 44 e 134 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 134 giorni dopo la scadenza

.pw (Palau)

Return to index

Il file.pw era originariamente riservato ai residenti di Palau, un paese insulare nella subregione della Micronesia dell'Oceania nel Pacifico occidentale, tuttavia ora è comunemente usato per rappresentare il «Web professionale» ed è disponibile per tutti.

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Protezione della privacy (si applica a tutti i tipi di contatto: persona, azienda, associazione e organismo pubblico)

Tutte le informazioni sono nascoste, tranne il nome dell'organizzazione.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza

- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 75 giorni dopo la scadenza

.qa (Qatar)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .qa o trasferire domini .qa a Route 53. Continueremo a supportare i domini .qa che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Da uno a cinque anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .qa a Route 53.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: no

- Il dominio viene eliminato dal record: 31 giorni dopo la scadenza

.ru (Federazione russa)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .ru o trasferire domini .ru a Route 53. Continueremo a supportare i domini .ru che sono già registrati con Route 53.

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

> **Note**
>
> Il record dei domini .ru domini aggiorna la data di scadenza per un dominio il giorno che il scade. Le query WHOIS mostrano la vecchia data di scadenza per il dominio fino a tale data indipendentemente dal quando si rinnova il dominio con Route 53.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Gli individui potrebbero dover fornire un numero di passaporto o il numero di carta di identità emessa dal governo.
- Per le aziende estere potrebbe essere necessario fornire un ID aziendale o di registrazione dell'azienda.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS

SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .ru a Route 53.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a 2 giorni prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 2 giorni prima della scadenza
- Il ripristino con il record è possibile: tra 2 giorni prima e 28 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 28 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .ru non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.sg (Repubblica di Singapore)

> **Important**
>
> Non è più possibile utilizzare Route 53 per registrare nuovi domini .sg o trasferire domini .sg a Route 53. Continueremo a supportare i domini .sg che sono già registrati con Route 53.

Return to index

Periodo di rinnovo

Uno o due anni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Non supportato. Non è più possibile trasferire domini .sg a Route 53.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 60 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .sg non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

Europa

Puoi utilizzare i seguenti domini di primo livello (TLDs) per l'Europa per registrare domini con Amazon Route 53.

, , , , , , , , , , , , , , , , , , , ,

Return to index

.be (Belgio)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì. È possibile ottenere il codice di trasferimento dal sito Web di DNS Belgio.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: alla data di scadenza
- Il ripristino con il record è possibile: fino a 40 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 40 giorni dopo la scadenza

.berlin (città di Berlino in Germania)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Il proprietario, il contatto amministrativo o tecnico deve fornire un indirizzo a Berlino, e il contatto amministrativo deve essere un singolo.
- È necessario attivare e utilizzare il dominio .berlin entro 12 mesi dalla registrazione (si applica a un sito Web, al reindirizzamento o all'indirizzo e-mail).
- Se si pubblica un sito Web utilizzando il dominio .berlin, oppure se il dominio .berlin reindirizza a un altro sito Web, i contenuti del sito Web devono essere correlati a Berlino.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per latino e cirillico.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 80 giorni dopo la scadenza

.ch (Svizzera)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 9 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 9 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 9 e 49 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 49 giorni dopo la scadenza

.co.uk (Regno Unito)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Se stai trasferendo un dominio .co.uk a Route 53, non devi ottenere un codice di autorizzazione. Puoi invece utilizzare il metodo fornito dal registrar del dominio attuale per aggiornare il valore del tag IPS per il dominio a GANDI, tutte lettere maiuscole. (Un tag IPS è richiesto da Nominet, il record per i nomi di dominio .uk.) Se il tuo registrar non modifica il valore del tag IPS, contatta Nominet.

> **Note**
>
> Quando si registra un dominio .co.uk, Route 53 imposta automaticamente il tag IPS per il dominio su GANDI.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 180 giorni prima e 30 giorni dopo la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: tra 30 e 90 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 90 giorni dopo la scadenza
- Il ripristino con il record è possibile: no

- Il dominio viene eliminato dal record: 92 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .co.uk non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.cz (Repubblica Ceca)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato, ma l'indirizzo e-mail e il numero di telefono sono nascosti per tutti i contatti.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

Se il tuo attuale registrar non fornisce un codice di autorizzazione, visita `https://www.nic.cz/whois/send-password/` per richiedere al registro dei domini CZ di inviarlo all'indirizzo e-mail del registrante.

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza

- Il rinnovo tardivo con Route 53 è possibile: fino a 58 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 59 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 60 giorni dopo la scadenza

.de (Germania)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- È necessario risiedere in Germania o disporre di un contatto fisico amministrativo (persona) che risiede in Germania e ha un indirizzo diverso da una casella postale.
- Durante la registrazione, il DNS (A, MX e CNAME) del nome di dominio deve essere configurato correttamente per poter superare il record di controllo di zona. Tre server di due diverse classi C sono necessarie.
- Se si utilizza un servizio DNS diverso da Route 53, i server dei nomi per il dominio dovranno superare un controllo per essere certi che siano configurati correttamente. Per determinare se i name server del tuo dominio supereranno il controllo, consulta https://www.denic. de/en/service/tools/nast/.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: alla data di scadenza
- Il ripristino con il record è possibile: contatta AWS Support.
- Il dominio viene eliminato dal record: contatta AWS Support.

.es (Spagna)

Return to index

Acquisto o trasferimento del dominio

> **Important**
>
> Al momento puoi acquistare nuovi nomi di dominio.es o trasferire domini.es su Route 53. Il tipo di contatto per il contatto del registrante non ha restrizioni. Il tipo di contatto amministrativo/tecnico/di fatturazione deve essere una persona.

Periodo di locazione della registrazione e rinnovo

Da uno a cinque anni.

Restrizioni

Aperto al pubblico, per coloro che hanno un interesse o una connessione con la Spagna.

Dal 2016, i registranti del dominio .ES sono tenuti a fornire un'e-mail di contatto del registrant. Se non hai fornito tali informazioni, devi farlo presso il registrar corrente prima di trasferire il dominio su Route 53.

Sono necessarie le seguenti informazioni:

- Identificatore ESNIC simile a. *AAAA0-ESNIC-F0*
- Se non conosci l'identificatore ESNIC, puoi ottenerlo dal registrar corrente. Il registrar è disponibile all'indirizzo: https://www.dominios.es/en.

A seconda che ricordi o meno la password presso il registrar, puoi scegliere una delle procedure seguenti per aggiornare l'indirizzo e-mail del registrant:

- Se ricordi la password, accedi a https://www.nic. es/sgnd/login.action utilizzando gli identificativi e la password ESNIC.

  Dopo aver effettuato l'accesso, puoi modificare il contatto e-mail del registrant scegliendo la scheda Modifica nella pagina del registro.
- Se hai dimenticato la password, accedi a https://www.nic. es/sgnd/peticion/editCorreo.azione?request_locale=it.

  Compila il modulo con l'identificativo ESNIC e il contatto e-mail del registrant nuovo e valido. Quindi, convalida il modulo scegliendo Elaborazione senza eID/certificato e carica il documento di identità richiesto.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

Il registro.es gestisce il codice di autorizzazione con a time-to-live e potrebbe scadere. Puoi aggiornare il codice di autenticazione rimuovendo lo stato transfer lock (clientTransferProhibited) dal tuo dominio, se presente. Se il dominio non ha alcun blocco di trasferimento, puoi aggiornare il codice di autenticazione attivandolo prima e poi disattivandolo.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a 6 giorni prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 6 giorni prima della scadenza
- Il ripristino con il record è possibile: tra 6 giorni prima e 4 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 4 giorni dopo la scadenza

.eu (Unione europea)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con una restrizione:

- Devi fornire un indirizzo postale valido da uno dei 30 stati dello Spazio economico europeo (SEE) oppure, se sei cittadino di uno dei 27 Stati membri dell'Unione europea (UE), devi specificare il tuo paese di cittadinanza dell'UE.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione API. RetrieveDomainAuthCode (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

Puoi anche generare il codice di autenticazione utilizzando il pannello «My.eu» nel registro: https://my.eurid.eu/.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: alla data di scadenza
- Il ripristino con il record è possibile: fino a 40 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 40 giorni dopo la scadenza

Ricerca WHOIS

Per informazioni sui domini .eu esistenti, consulta https://whois.eurid.eu/en/.

.fi (Finlandia)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a cinque anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- L'estensione .fi è disponibile per gli individui che hanno domicilio in Finlandia e dispongono di un numero di identità finlandese e persone giuridiche o privati imprenditori registrati in Finlandia.
- Se l'indirizzo di contatto del registrante si trova in Finlandia, è richiesto il numero di identità finlandese per un singolo registrante e il numero di società finlandese per il registrante della società. Inoltre, durante la registrazione è necessario fornire le seguenti informazioni:
  - Se il contatto è basato su una persona fisica o morale in Finlandia.
  - L'identificatore del record in cui il nome viene registrato, se basato su un nome di persona morale.
  - Il numero del record nel record in cui il nome viene registrato, se basato su un nome di persona morale.

- Il numero di identificazione per una persona morale in Finlandia.
- Il numero di identificazione per una persona fisica in Finlandia.
- Se il dichiarante non è una società finlandese, è necessario fornire il numero aziendale come numero di partita IVA.

- Se l'indirizzo del registrante non si trova in Finlandia, non è richiesto alcun numero di identità o di società finlandese.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'API. RetrieveDomainAuthCode (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: no

Eliminazione della registrazione di dominio

Per ulteriori informazioni sull'eliminazione dei domini, consulta Eliminazione della registrazione di un nome di dominio.

.fr (Francia)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Le persone devono avere almeno 18 anni e devono fornire il propriodate-of-birth.
- Le aziende devono essere situate nell'Area economica europea o in Svizzera.
- Le aziende devono compilare tutti i campi di identificazione dell'azienda (numero di registrazione IVA, SIREN, WALDEC, DUNS e così via), poiché questo faciliterà qualsiasi verifica che AFNIC può eseguire in un secondo momento.
- Le stesse condizioni di idoneità sono applicabili al contatto a livello amministrativo.
- I nomi e le condizioni sono soggetti a una revisione dell'AFNIC (articolo 2.4 dello statuto di denominazione) e alle seguenti condizioni supplementari:
  - I nomi di dominio precedentemente riservati o vietati sono aperti ai richiedenti che giustificano un diritto legittimo e agiscono in buona fede.
  - I nomi che iniziano con ville, mairie, agglo, cc, cg e cr sono soggetti alle convenzioni di denominazione di AFNIC.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 27 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 28 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 28 e 58 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 58 giorni dopo la scadenza

.gg (Guernsey)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 35 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 35 giorni dopo la scadenza

.im (Isola di Man)

Utilizzato anche come TLD generico, spesso dai servizi di messaggistica istantanea o da coloro che desiderano sviluppare un marchio personale di tipo "I am".

Return to index

Periodo di locazione della registrazione e rinnovo

Uno o due anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza

- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 30 giorni dopo la scadenza

.it (Italia)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Gli individui o aziende devono avere un indirizzo registrato nell'Unione europea.
- Se il paese di origine è l'Italia, è necessario immettere un codice fiscale. Se il paese di origine è nell'Unione europea, è necessario inserire un numero di documento di identità (ID).
- Se si specifica Company (Azienda), Association (Associazione) o Public body (Ente pubblico) per il tipo di contatto, occorre un numero di partita IVA.
- I server di nomi per il tuo dominio devono superare un controllo DNS. Ti consigliamo di controllare i server dei nomi all'indirizzo https://dns-check.nic.it/ prima di inviare la richiesta di modifica. Se il nome di dominio non è conforme ai requisiti tecnici (ad esempio non è associato a un server dei nomi operativo) e non viene corretto entro 30 giorni, il tuo nome di dominio verrà eliminato dal record. Non emettiamo rimborsi per domini che vengono eliminati perché non soddisfano i requisiti tecnici.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Non supportato.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 13 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 49 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 14 e 44 giorni dopo la scadenza
- Il dominio viene eliminato dal record: contatta AWS Support.

.me (Montenegro)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Domain.me, record per domini .me, considera nomi di dominio di due lettere e alcuni nomi di dominio più lunghi come nomi di dominio premium. Non è possibile eseguire la registrazione di domini premium .me o trasferirli a Route 53. Per ulteriori informazioni sui nomi di dominio premium .me, consulta il sito Web domain.me.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per arabo, bielorusso, bosniaco, bulgaro, cinese semplificato, cinese tradizionale, croato, danese, francese, tedesco, hindi, ungherese, islandese, italiano, coreano, lettone, lituano, mongolo, montenegrino, polacco, portoghese, russo, serbo, spagnolo, svedese, turco e ucraino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 29 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 30 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 30 e 60 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 65 giorni dopo la scadenza

.me.uk (Regno Unito)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Se stai trasferendo un dominio .me.uk a Route 53, non devi ottenere un codice di autorizzazione. Puoi invece utilizzare il metodo fornito dal registrar del dominio attuale per aggiornare il valore del tag IPS per il dominio a GANDI, tutte lettere maiuscole. (Un tag IPS è richiesto da Nominet,

il record per i nomi di dominio .uk.) Se il tuo registrar non modifica il valore del tag IPS, contatta Nominet.

> **Note**
>
> Quando si registra un dominio .me.uk, Route 53 imposta automaticamente il tag IPS per il dominio su GANDI.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 180 giorni prima e 30 giorni dopo la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: tra 30 e 90 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 90 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 92 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .me.uk non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.nl (Paesi Bassi)

Return to index

Periodo di locazione della registrazione e rinnovo

Un anno.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Il proprietario o il contatto amministrativo devono fornire un indirizzo valido nei Paesi Bassi. Una presenza locale è obbligatoria.

- Se non si dispone di un indirizzo valido nei Paesi Bassi, il Registry SIDN fornirà un indirizzo di domicilio secondo la procedura pertinente.
- La lunghezza del nome del dominio deve essere compresa tra 3 e 63 caratteri, escluso .nl.

Protezione della privacy

Determinato dal record.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a 1 giorno prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 1 giorno prima della scadenza
- Il ripristino con il record è possibile: tra 1 giorno prima e 39 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 39 giorni dopo la scadenza

.org.uk (Regno Unito)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Se stai trasferendo un dominio .org.uk a Route 53, non devi ottenere un codice di autorizzazione. Puoi invece utilizzare il metodo fornito dal registrar del dominio attuale per aggiornare il valore del tag IPS per il dominio a GANDI, tutte lettere maiuscole. (Un tag IPS è richiesto da Nominet, il record per i nomi di dominio .uk.) Se il tuo registrar non modifica il valore del tag IPS, contatta Nominet.

> **Note**
>
> Quando si registra un dominio .org.uk, Route 53 imposta automaticamente il tag IPS per il dominio su GANDI.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 180 giorni prima e 30 giorni dopo la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: tra 30 e 90 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 90 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 92 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .org.uk non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.ruhr (regione della Ruhr, parte occidentale della Germania)

Return to index

L'estensione .ruhr è per la regione della Ruhr (parte occidentale della Germania).

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con una restrizione:

- Il contatto amministrativo deve essere una persona che dispone di un indirizzo in Germania.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato (ä, ö, ü, ß).

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza

- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: contatta AWS Support.

.se (Sweden)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Se ti trovi in Svezia, devi fornire un numero di identità svedese valido. Il formato del numero ID èYYMMDD-NNNN.
- Se ti trovi al di fuori di Svezia, devi inserire un numero di ID valido, ad esempio un codice fiscale.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Non supportato. Ti consigliamo di prevenire i trasferimenti non autorizzati limitando l'accesso all'azione dell'RetrieveDomainAuthCodeAPI. (Quando limiti l'accesso a questa API Route 53, limiti anche chi può generare un codice di autorizzazione utilizzando la console Route 53 e altri AWS SDKs metodi programmatici). Per ulteriori informazioni, consulta Identity and Access Management in Amazon Route 53.

Nomi di dominio internazionalizzati

Supportato per latino, svedese e yiddish.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino a 1 giorno prima della data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: No
- Il dominio viene eliminato da Route 53: 1 giorno prima della scadenza
- Il ripristino con il record è possibile: tra 1 giorno prima e 59 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 64 giorni dopo la scadenza

.uk (United Kingdom)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, senza restrizioni.

Protezione della privacy

Tutte le informazioni sono nascoste.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato

Nomi di dominio internazionalizzati

Non supportato.

Codice di autorizzazione richiesto per i trasferimenti

Se stai trasferendo un dominio .uk a Route 53, non devi ottenere un codice di autorizzazione. Puoi invece utilizzare il metodo fornito dal registrar del dominio attuale per aggiornare il valore del tag IPS per il dominio a GANDI, tutte lettere maiuscole. (Un tag IPS è richiesto da Nominet, il record per i nomi di dominio .uk.) Se il tuo registrar non modifica il valore del tag IPS, contatta Nominet.

> **Note**
>
> Quando si registra un dominio .uk, Route 53 imposta automaticamente il tag IPS per il dominio su GANDI.

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: tra 180 giorni prima e 30 giorni dopo la data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: tra 30 e 90 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 90 giorni dopo la scadenza
- Il ripristino con il record è possibile: no
- Il dominio viene eliminato dal record: 92 giorni dopo la scadenza

Eliminazione della registrazione di dominio

Il record per domini .uk non consente di eliminare registrazioni di domini. Al contrario, è necessario disabilitare il rinnovo automatico e attendere che il dominio scada. Per ulteriori informazioni, consulta Eliminazione della registrazione di un nome di dominio.

.wien (città di Vienna in Austria)

Return to index

Periodo di locazione della registrazione e rinnovo

Da uno a dieci anni.

Restrizioni

Aperto al pubblico, con alcune restrizioni:

- Devi mostrare una affinità economica, culturale, turistica, storica, sociale o di altro tipo con la città di Vienna in Austria.
- Il nome di dominio .wien deve essere utilizzato in connessione con le condizioni sopra indicate, per tutta la durata della registrazione.

Protezione della privacy

Non supportato.

Blocco dei domini per evitare trasferimenti non autorizzati

Supportato.

Nomi di dominio internazionalizzati

Supportato per il latino.

Codice di autorizzazione richiesto per i trasferimenti

Sì

DNSSEC

Supportato per la registrazione del dominio. Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

Scadenze per il rinnovo e il ripristino dei domini

- Il rinnovo è possibile: fino alla data di scadenza
- Il rinnovo tardivo con Route 53 è possibile: fino a 44 giorni dopo la scadenza
- Il dominio viene eliminato da Route 53: 45 giorni dopo la scadenza
- Il ripristino con il record è possibile: tra 45 e 75 giorni dopo la scadenza
- Il dominio viene eliminato dal record: 80 giorni dopo la scadenza

Configurazione di Amazon Route 53 come servizio DNS

Puoi utilizzare Amazon Route 53 come servizio DNS per il dominio, ad esempio esempio.com. Se Route 53 è il tuo servizio DNS, instrada il traffico Internet al tuo sito Web traducendo i nomi dominio brevi, ad esempio www.esempio.com, in indirizzi IP numerici come 192.0.2.1, che i computer utilizzano per connettersi tra loro. Quando un utente digita il tuo nome dominio in un browser oppure invia un'e-mail, una query DNS viene inoltrata a Route 53, che risponde con il valore appropriato. Ad esempio, Route 53 potrebbe rispondere con l'indirizzo IP del server Web per esempio.com.

In questo capitolo verrà illustrato come configurare Route 53 per instradare il traffico Internet in modo corretto. Spiegheremo inoltre come migrare il servizio DNS a Route 53 se si sta utilizzando un altro servizio DNS e come utilizzare Route 53 come servizio DNS per un nuovo dominio.

Argomenti

Rendere Amazon Route 53 il servizio DNS per un dominio esistente

Se stai trasferendo una o più registrazioni di dominio a Route 53 e al momento utilizzi un registrar del dominio che non offre un servizio DNS pagato, devi migrare il servizio DNS prima di migrare il dominio. In caso contrario, il registrar smetterà di fornire il servizio DNS durante il trasferimento dei domini e i siti Web e le applicazioni associate diventeranno non disponibili su Internet. Puoi migrare il servizio DNS anche dal registrar corrente a un altro fornitore di servizi DNS. Non è necessario utilizzare Route 53 come provider del servizio DNS per i domini registrati con Route 53.

Il processo dipende dall'utilizzo o meno del dominio:

- Se il dominio attualmente riceve traffico, ad esempio se gli utenti utilizzano il nome di dominio per navigare in un sito Web o accedere a un'applicazione Web, consulta Rendere Route 53 il servizio DNS per un dominio in uso.
- Se il dominio non riceve traffico (o riceve pochissimo traffico), consulta Rendere Route 53 il servizio DNS per un dominio non attivo.

Per entrambe le opzioni, il tuo dominio dovrebbe rimanere disponibile durante l'intero processo di migrazione. Tuttavia, nell'improbabile caso in cui ci siano problemi, la prima opzione ti consente di eseguire il rollback della migrazione in modo rapido. Con la seconda opzione, il tuo dominio potrebbe non essere disponibile per un paio di giorni.

Se desideri metterti in contatto con un esperto di AWS, visita l'assistenza alle vendite.

Rendere Route 53 il servizio DNS per un dominio in uso

Se desideri eseguire la migrazione del servizio DNS ad Amazon Route 53 per un dominio che attualmente riceve traffico, ad esempio se gli utenti utilizzano il nome di dominio per navigare in un sito Web o accedere a un'applicazione Web, esegui le procedure descritte in questa sezione.

Argomenti

Fase 1: ottieni la tua attuale configurazione DNS dal fornitore di servizi DNS attuale (facoltativo ma consigliato)

Quando esegui la migrazione del servizio DNS da un altro provider a Route 53, riproduci la configurazione DNS corrente in Route 53. In Route 53, è necessario creare una zona ospitata con lo stesso nome di dominio e creare i record nella zona ospitata. Ogni record indica il modo in cui desideri instradare il traffico per un determinato nome di dominio o di sottodominio. Ad esempio, quando qualcuno inserisce il tuo nome di dominio in un browser Web, desideri che il traffico venga indirizzato a un server Web nel tuo data center, a un' EC2 istanza Amazon, a una CloudFront distribuzione o a qualche altra posizione?

Il processo che usi dipende dalla complessità della tua attuale configurazione DNS:

- Se la tua attuale configurazione DNS è semplice: se stai instradando il traffico Internet per pochi sottodomini a un piccolo numero di risorse, come server Web o bucket Amazon S3, puoi creare manualmente alcuni record nella console Route 53.
- Se la configurazione DNS corrente è più complessa e desideri solo riprodurre la configurazione corrente: puoi semplificare la migrazione se puoi ottenere un file di zona dal provider di servizi DNS corrente e importare il file di zona in Route 53. (Non tutti i fornitori di servizi DNS offrono i file di zona.) Quando importi un file di zona, Route 53 riproduce automaticamente la configurazione esistente creando i record corrispondenti nella tua zona ospitata.

  Prova a chiedere al servizio clienti del tuo attuale fornitore di servizi DNS come ottenere un file di zona o un elenco di record. Per informazioni sul formato richiesto per il file di zona, consulta Creazione di record mediante importazione di un file di zona.
- Se la tua attuale configurazione DNS è più complessa e sei interessato alle caratteristiche di routing di Route 53: esamina la seguente documentazione per vedere se desideri utilizzare le funzionalità di Route 53 che non sono disponibili da altri fornitori di servizi DNS. In questo caso, puoi creare record manualmente oppure importare un file di zona e quindi creare o aggiornare i record più tardi:
  - Scelta tra record alias e non aliasspiega i vantaggi dei record di alias Route 53, che indirizzano il traffico verso alcune AWS risorse, come CloudFront distribuzioni e bucket Amazon S3, gratuitamente.
  - Scegliere una policy di routing spiega le opzioni di routing di Route 53, ad esempio routing in base alla posizione degli utenti, routing in base alla latenza tra gli utenti e le risorse, routing in base all'integrità delle risorse e routing alle risorse in base ai pesi specificati.

> **Note**
>
> Puoi anche importare un file di zona e successivamente modificare la configurazione per usufruire dei record alias e di policy di routing complesse.

Se non sei in grado di ottenere un file di zona o se desideri creare manualmente record in Route 53, i record che molto probabilmente dovrai migrare includono i seguenti:

- Record A (Indirizzo): associa un nome di dominio o un nome di sottodominio all' IPv4 indirizzo (ad esempio, 192.0.2.3) della risorsa corrispondente
- Record AAAA (Indirizzo): associano un nome di dominio o un nome di sottodominio all' IPv6 indirizzo (ad esempio, 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) della risorsa corrispondente
- Record di server di posta (MX): instradano il traffico ai server di posta
- Record CNAME: reinstradano il traffico per un nome di dominio (esempio.net) a un altro nome di dominio (esempio.com)
- Record per altri tipi di record DNS supportati: per un elenco dei tipi di record supportati, consulta Tipi di record DNS supportati.

Fase 2: crea una zona ospitata

Per indicare ad Amazon Route 53 come desideri instradare il traffico per il tuo dominio, crea una zona ospitata che ha lo stesso nome del tuo dominio, quindi crea i record nella zona ospitata.

> **Important**
>
> Puoi creare una zona ospitata solo per un dominio che si dispone dell'autorizzazione per amministrare. Normalmente, questo significa che sei proprietario del dominio, ma potresti anche sviluppare un'applicazione per il registrant del dominio.

Quando si crea una zona ospitata, Route 53 crea automaticamente un record di server di nomi (NS) e un record di origine di autorità (SOA) per la zona. Il record NS identifica il nome dei quattro server dei nomi che Route 53 ha associato alla tua zona ospitata. Per rendere Route 53 il servizio DNS per il tuo dominio, devi aggiornare la registrazione per il dominio in modo da utilizzare questi quattro server dei nomi.

> **Important**
>
> Non creare ulteriori record di server dei nomi (NS) o origine di autorità (SOA) e non eliminare i record SOA e NS esistenti.

Per creare una zona ospitata

1. Accedi AWS Management Console e https://console.aws.amazon.com/route53/apri la console Route 53 all'indirizzo.
2. Se sei nuovo di Route 53, scegli Nozioni di basein Gestione DNS e scegli Crea zone ospitate.

   Se stai già utilizzando Route 53, scegli Zone ospitate nel pannello di navigazione, quindi scegli Crea zone ospitate.
3. Nel riquadro Crea zona ospitata, inserisci un nome di dominio e, facoltativamente, un commento. Per ulteriori informazioni su un'impostazione, apri il pannello della guida sul lato destro.

   Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.
4. Per Tipo, accetta il valore di default di Zona ospitata pubblica.
5. Scegli Crea zona ospitata.

Fase 3: crea i record

Una volta creata una zona ospitata, è necessario creare record nella stessa che definiscono il punto in cui si desidera instradare il traffico per un dominio (esempio.com) o sottodominio (www.esempio.com). Ad esempio, se desideri indirizzare il traffico per example.com e www.example.com verso un server Web su un' EC2 istanza Amazon, crei due record, uno denominato example.com e l'altro denominato www.example.com. In ogni record, specifichi l'indirizzo IP dell'istanza. EC2

Puoi creare record in diversi modi:

Importa un file di zona

Questo è il metodo più semplice se hai ottenuto un file di zona dal servizio DNS corrente in Fase 1: ottieni la tua attuale configurazione DNS dal fornitore di servizi DNS attuale (facoltativo ma

consigliato). Amazon Route 53 non è in grado di prevedere quando creare record alias o utilizzare tipi di routing speciali, ad esempio ponderati o di failover. Di conseguenza, se importi un file di zona, Route 53 crea record DNS standard mediante la policy di routing semplice.

Per ulteriori informazioni, consulta Creazione di record mediante importazione di un file di zona.

Crea record individualmente nella console

Se non hai ottenuto un file di zona e desideri creare solo pochi record con una policy di routing semplice per iniziare, puoi creare i record nella console Route 53. Puoi creare sia record alias che non alias.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Scegliere una policy di routing
- Scelta tra record alias e non alias
- Creazione di record utilizzando la console Amazon Route 53

Crea record a livello programmatico

È possibile creare record utilizzando uno dei AWS SDKs AWS CLI, o AWS Tools for Windows PowerShell. Per ulteriori informazioni, consulta la documentazione di AWS.

Se utilizzi un linguaggio di programmazione che AWS non fornisce un SDK per, puoi anche utilizzare l'API Route 53. Per ulteriori informazioni, consulta il riferimento API di Amazon Route 53.

Fase 4: riduzione delle impostazioni TTL

L'impostazione TTL (time-to-live) per un record consente di specificare il periodo di tempo per cui desideri che il resolver DNS memorizzi nella cache i record e utilizzi le informazioni memorizzate nella cache. Quando il TTL scade, un resolver invia un'altra query al fornitore di servizi DNS per un dominio per ottenere le informazioni più recenti.

L'impostazione TTL tipica per il record NS è 172800 secondi, o due giorni. Il record NS elenca i server dei nomi che il Domain Name System (DNS) può utilizzare per ottenere informazioni su come instradare il traffico per il tuo dominio. Abbassando il valore TTL per il record NS, sia con il tuo provider del servizio DNS corrente sia con Amazon Route 53, riduci i tempi di inattività per il dominio se rilevi un problema durante la migrazione del DNS a Route 53. Se non riduci il TTL, il tuo dominio potrebbe essere non disponibile su Internet per un massimo di due giorni in caso di problemi.

> **Note**
>
> Alcuni risolutori completi possono memorizzare nella cache il TTL del record NS del server autorevole padre, per cui è necessario anche ridurre il TTL dei record NS registrati sul server DNS autorevole padre.

È consigliabile modificare il TTL nei seguenti record NS:

- Nel record NS nella zona ospitata per l'attuale fornitore di servizi DNS. (Il tuo attuale fornitore potrebbe utilizzare una terminologia diversa).
- Nel record NS nella zona ospitata creata in Fase 2: crea una zona ospitata.

Per ridurre il TTL nel record NS con l'attuale fornitore di servizi DNS

- Utilizza il metodo fornito dall'attuale fornitore di servizi DNS per il dominio per modificare il valore TTL per il record NS nella zona ospitata per il tuo dominio.

Come ridurre l'impostazione TTL sul record NS in una zona ospitata di Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Seleziona Hosted Zones (Zone ospitate) nel pannello di navigazione.
3. Scegli il nome della zona ospitata.
4. Scegli il record NS, quindi Modifica.
5. Modifica il valore di TTL (secondi). È consigliabile specificare un valore compreso tra 60 secondi e 900 secondi (15 minuti).
6. Scegli Save changes (Salva modifiche).

Fase 5: (Se è stato configurato DNSSEC) Rimozione del record DS dalla zona padre

Se hai configurato DNSSEC per il dominio, prima di eseguire la migrazione del dominio a Route 53 rimuovi il record Delegation Signer (DS) dalla zona padre.

Se la zona padre è ospitata tramite Route 53 o un altro registrar, contattalo per rimuovere il record DS.

Poiché al momento non è possibile abilitare la firma DNSSEC su due provider, è necessario rimuovere qualsiasi DS o DNSKEYs disattivare DNSSEC. Questo segnala temporaneamente ai resolver DNS di disabilitare la convalida DNSSEC. Nella Fase 11, potrai riabilitare la convalida DNSSEC, se lo desideri, dopo aver completato la transizione a Route 53.

Per ulteriori informazioni, consulta Eliminazione di chiavi pubbliche per un dominio.

Fase 6: Attendi la scadenza del vecchio TTL

Se il dominio è in uso, per esempio se gli utenti utilizzano il nome di dominio per navigare in un sito Web o accedere a un'applicazione Web, allora i resolver DNS hanno memorizzato nella cache i nomi del server dei nomi che sono stati fornito dal tuo provider di servizi DNS corrente. Un resolver DNS che ha memorizzato nella cache tali informazioni da pochi minuti, le salverà per quasi due giorni aggiuntivi.

Per garantire che la migrazione del servizio DNS a Route 53 avvenga in una sola volta, attendi due giorni dopo aver abbassato il TTL. Dopo che il TTL di due giorni scade e i resolver richiedono i server di nomi per il tuo dominio, i resolver otterranno i server dei nomi attuali e il nuovo TTL che hai specificato in Fase 4: riduzione delle impostazioni TTL.

Fase 7: Aggiornamento dei record NS per utilizzare i server dei nomi di Route 53

Per iniziare a utilizzare Amazon Route 53 come servizio DNS per un dominio, utilizzare il metodo fornito dal provider di servizi DNS corrente per sostituire i server dei nomi correnti nel record NS con i server dei nomi Route 53.

> **Note**
>
> Quando si aggiorna il record NS con il provider di servizi DNS corrente per utilizzare i server dei nomi di Route 53, si sta aggiornando la configurazione DNS per il dominio. (Ciò è paragonabile all'aggiornamento del record NS nella zona ospitata Route 53 per un dominio, tranne che stai aggiornando l'impostazione con il servizio DNS da cui stai effettuando la migrazione.)

Come aggiornare il record NS nel registrar, o nella zona padre, per utilizzare i server dei nomi di Route 53

1. Nella console Route 53, ottieni i server dei nomi per la tua zona ospitata:

a. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/

b. Nel pannello di navigazione, scegli Zone ospitate.

c. Nella pagina Zone ospitate, scegli il nome per la zona ospitata applicabile.

d. Prendi nota dei quattro nomi indicati per Server dei nomi nella sezione Dettagli della zona ospitata.

2. Utilizza il metodo che viene fornito dall'attuale servizio DNS per il dominio per aggiornare il record NS per la zona ospitata. Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio. Il processo dipende dal fatto che il servizio DNS corrente ti consenta o meno di eliminare i server dei nomi:

   Se si è in grado di eliminare i nomi dei server

   - Annota i server dei nomi correnti nel record NS per la zona ospitata. Se hai bisogno di ripristinare l'attuale configurazione DNS, questi sono i server che dovrai specificare.
   - Elimina gli attuali server dei nomi dal record NS.
   - Aggiorna il record NS con i nomi di tutti e quattro i server dei nomi di Route 53 ottenuti nella fase 1 di questa procedura.

   > **Note**
   >
   > Al termine, i soli server dei nomi nel record NS saranno i quattro server dei nomi di Route 53.

   Se puoi eliminare i nomi dei server

   - Scegli la possibilità di utilizzare i server dei nomi personalizzati.
   - Aggiungi tutti e quattro i server dei nomi di Route 53 ottenuti nella fase 1 di questa procedura.

Fase 8: Monitoraggio del traffico per il dominio

Monitora il traffico per il dominio, tra cui il traffico di applicazioni e siti Web o e-mail:

- Se il traffico rallenta o si interrompe: utilizza il metodo fornito dal servizio DNS precedente per modificare i server di nomi per il dominio e riportarli ai precedenti server di nomi. Questi sono i

server dei nomi che avevi annotato nella fase 7 di Come aggiornare il record NS nel registrar, o nella zona padre, per utilizzare i server dei nomi di Route 53. Stabilisci quindi ciò che non ha funzionato.

- Se il traffico non è influenzato: passa a Fase 9: modifica il TTL per il record NS riportandolo a un valore superiore.

Fase 9: modifica il TTL per il record NS riportandolo a un valore superiore

Nella zona ospitata di Amazon Route 53 per il dominio, cambia il valore TTL per il record NS con un valore più tipico, per esempio, 172.800 secondi (due giorni). Questo migliora la latenza per gli utenti, perché non dovranno aspettare, come spesso accade per resolver DNS, per inviare una query per i server dei nomi per il tuo dominio.

Come modificare il valore TTL per il record NS nella zona ospitata di Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Seleziona Hosted Zones (Zone ospitate) nel pannello di navigazione.
3. Scegli il nome della zona ospitata.
4. Nell'elenco dei record per la zona ospitata, scegli il record NS.
5. Scegli Modifica.
6. Modifica TTL (secondi) nel numero di secondi in cui desideri che il resolver DNS memorizzi i nomi dei server dei nomi per il tuo dominio. Consigliamo un valore di 172800 secondi.
7. Scegli Save changes (Salva modifiche).

Fase 10: Trasferimento della registrazione del dominio ad Amazon Route 53

Ora che hai trasferito il servizio DNS per un dominio ad Amazon Route 53, puoi facoltativamente trasferire la registrazione per il dominio a Route 53. Per ulteriori informazioni, consulta Trasferimento della registrazione per un dominio ad Amazon Route 53.

Fase 11: Riabilitazione della firma DNSSEC (se necessario)

Ora che hai trasferito il servizio DNS per un dominio ad Amazon Route 53, puoi riabilitare la firma DNSSEC.

L'abilitazione della firma DNSSEC prevede due fasi:

- Passaggio 1: abilita la firma DNSSEC per Route 53 e richiedi che Route 53 crei una chiave di firma delle chiavi (KSK) basata su una chiave gestita dal cliente (). AWS Key Management Service AWS KMS
- Fase 2: Creazione di una catena di attendibilità per la zona ospitata aggiungendo un record Delegation Signer (DS) alla zona padre, in modo che le risposte DNS possano essere autenticate con firme crittografiche attendibili.

  Per istruzioni, consulta Abilitazione della firma DNSSEC e creazione di una catena di attendibilità.

Rendere Route 53 il servizio DNS per un dominio non attivo

Se desideri eseguire la migrazione del servizio DNS a Amazon Route 53 per un dominio che non riceve ancora traffico (o che ne riceve pochissimo), esegui le procedure descritte in questa sezione.

Argomenti

Fase 1: ottieni la tua attuale configurazione DNS dal fornitore di servizi DNS attuale (domini inattivi)

Quando esegui la migrazione del servizio DNS da un altro provider a Route 53, riproduci la configurazione DNS corrente in Route 53. In Route 53, è necessario creare una zona ospitata con lo stesso nome di dominio e creare i record nella zona ospitata. Ogni record indica il modo in cui desideri instradare il traffico per un determinato nome di dominio o di sottodominio. Ad esempio, quando qualcuno inserisce il tuo nome di dominio in un browser Web, desideri che il traffico venga indirizzato a un server Web nel tuo data center, a un' EC2 istanza Amazon, a una CloudFront distribuzione o a qualche altra posizione?

Il processo che usi dipende dalla complessità della tua attuale configurazione DNS:

- Se la tua attuale configurazione DNS è semplice: se stai instradando il traffico Internet per pochi sottodomini a un piccolo numero di risorse, come server Web o bucket Amazon S3, puoi creare manualmente alcuni record nella console Route 53.

- Se la configurazione DNS corrente è più complessa e desideri solo riprodurre la configurazione corrente: puoi semplificare la migrazione se puoi ottenere un file di zona dal provider di servizi DNS corrente e importare il file di zona in Route 53. (Non tutti i fornitori di servizi DNS offrono i file di zona.) Quando importi un file di zona, Route 53 riproduce automaticamente la configurazione esistente creando i record corrispondenti nella tua zona ospitata.

  Prova a chiedere al servizio clienti del tuo attuale fornitore di servizi DNS come ottenere un file di zona o un elenco di record. Per informazioni sul formato richiesto per il file di zona, consulta Creazione di record mediante importazione di un file di zona.
- Se la tua attuale configurazione DNS è più complessa e sei interessato alle caratteristiche di routing di Route 53: esamina la seguente documentazione per vedere se desideri utilizzare le funzionalità di Route 53 che non sono disponibili da altri fornitori di servizi DNS. In questo caso, puoi creare record manualmente oppure importare un file di zona e quindi creare o aggiornare i record più tardi:
  - Scelta tra record alias e non aliasspiega i vantaggi dei record di alias Route 53, che indirizzano il traffico verso alcune AWS risorse, come CloudFront distribuzioni e bucket Amazon S3, gratuitamente.
  - Scegliere una policy di routing spiega le opzioni di routing di Route 53, ad esempio routing in base alla posizione degli utenti, routing in base alla latenza tra gli utenti e le risorse, routing in base all'integrità delle risorse e routing alle risorse in base ai pesi specificati.

> **Note**
>
> Puoi anche importare un file di zona e successivamente modificare la configurazione per usufruire dei record alias e di policy di routing complesse.

Se non sei in grado di ottenere un file di zona o se desideri creare manualmente record in Route 53, i record che molto probabilmente dovrai migrare includono i seguenti:

- Record A (Indirizzo): associa un nome di dominio o un nome di sottodominio all' IPv4 indirizzo (ad esempio, 192.0.2.3) della risorsa corrispondente
- Record AAAA (Indirizzo): associano un nome di dominio o un nome di sottodominio all' IPv6 indirizzo (ad esempio, 2001:0 db 8:85 a 3:0000:0000:abcd: 0001:2345) della risorsa corrispondente
- Record di server di posta (MX): instradano il traffico ai server di posta

- Record CNAME: reinstradano il traffico per un nome di dominio (esempio.net) a un altro nome di dominio (esempio.com)
- Record per altri tipi di record DNS supportati: per un elenco dei tipi di record supportati, consulta Tipi di record DNS supportati.

Fase 2: crea una zona ospitata (domini inattivi)

Per indicare ad Amazon Route 53 come desideri instradare il traffico per il tuo dominio, crea una zona ospitata che ha lo stesso nome del tuo dominio, quindi crea i record nella zona ospitata.

> **Important**
>
> Puoi creare una zona ospitata solo per un dominio che si dispone dell'autorizzazione per amministrare. Normalmente, questo significa che sei proprietario del dominio, ma potresti anche sviluppare un'applicazione per il registrant del dominio.

Quando si crea una zona ospitata, Route 53 crea automaticamente un record di server di nomi (NS) e un record di origine di autorità (SOA) per la zona. Il record NS identifica il nome dei quattro server dei nomi che Route 53 ha associato alla tua zona ospitata. Per rendere Route 53 il servizio DNS per il tuo dominio, devi aggiornare la registrazione per il dominio in modo da utilizzare questi quattro server dei nomi.

> **Important**
>
> Non creare ulteriori record di server dei nomi (NS) o origine di autorità (SOA) e non eliminare i record SOA e NS esistenti.

Per creare una zona ospitata

1. Accedi AWS Management Console e https://console.aws.amazon.com/route53/apri la console Route 53 all'indirizzo.
2. I nuovi utenti di Route 53 possono consultare Nozioni di base.

   Se stai già utilizzando Route 53, scegli Zone ospitate nel pannello di navigazione.
3. Scegli Crea zona ospitata.

4. Nel riquadro Crea zona ospitata, inserisci un nome di dominio e, facoltativamente, un commento. Per ulteriori informazioni su un'impostazione, posiziona il puntatore del mouse sulla rispettiva etichetta per visualizzare una descrizione.

   Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

5. Per Tipo di record, accetta il valore di default di Zona ospitata pubblica.
6. Scegli Crea zona ospitata.

Fase 3: crea i record (domini inattivi)

Una volta creata una zona ospitata, è necessario creare record nella stessa che definiscono il punto in cui si desidera instradare il traffico per un dominio (esempio.com) o sottodominio (www.esempio.com). Ad esempio, se desideri indirizzare il traffico per example.com e www.example.com verso un server Web su un' EC2 istanza Amazon, crei due record, uno denominato example.com e l'altro denominato www.example.com. In ogni record, specifichi l'indirizzo IP dell'istanza. EC2

Puoi creare record in diversi modi:

Importa un file di zona

Questo è il metodo più semplice se hai ottenuto un file di zona dal servizio DNS corrente in Fase 1: ottieni la tua attuale configurazione DNS dal fornitore di servizi DNS attuale (domini inattivi). Amazon Route 53 non è in grado di prevedere quando creare record alias o utilizzare tipi di routing speciali, ad esempio ponderati o di failover. Di conseguenza, se importi un file di zona, Route 53 crea record DNS standard mediante la policy di routing semplice.

Per ulteriori informazioni, consulta Creazione di record mediante importazione di un file di zona.

Crea record individualmente nella console

Se non hai ottenuto un file di zona e desideri creare solo pochi record con una policy di routing semplice per iniziare, puoi creare i record nella console Route 53. Puoi creare sia record alias che non alias.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Scegliere una policy di routing

- Scelta tra record alias e non alias
- Creazione di record utilizzando la console Amazon Route 53

Crea record a livello programmatico

È possibile creare record utilizzando uno dei AWS SDKs AWS CLI, o AWS Tools for Windows PowerShell. Per ulteriori informazioni, consulta la documentazione di AWS.

Se utilizzi un linguaggio di programmazione che AWS non fornisce un SDK per, puoi anche utilizzare l'API Route 53. Per ulteriori informazioni, consulta il riferimento API di Amazon Route 53.

Fase 4: Aggiornamento della registrazione del dominio per utilizzare server di nomi di Amazon Route 53 (domini inattivi)

Una volta completata la creazione di record per il dominio, è possibile modificare il servizio DNS per il dominio a Amazon Route 53. Esegui la seguente procedura per aggiornare le impostazioni con il registrar del dominio.

Per aggiornare i server dei nomi per il dominio

1. Nella console Route 53, recupera i server dei nomi per la tua zona ospitata Route 53
   a. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
   b. Nel pannello di navigazione, scegli Zone ospitate.
   c. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata, quindi seleziona Visualizza dettagli.
   d. Nella pagina dei dettagli della zona ospitata, scegli Dettagli della zona ospitata.
   e. Prendi nota dei quattro server indicati per Server dei nomi.
2. Utilizza il metodo fornito dal registrar del dominio per modificare i server dei nomi affinché il dominio utilizzi i quattro server dei nomi Route 53 ottenuti nella fase 2 di questa procedura.

   Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

Configurazione del routing DNS per un nuovo dominio

Un nuovo dominio acquistato da Route 53

Quando record un dominio con Route 53, Route 53 diventa automaticamente il servizio DNS per il dominio. Route 53 crea una zona ospitata con lo stesso nome del nome di dominio, assegna quattro server alla zona ospitata e aggiorna il dominio in modo da utilizzare tali server dei nomi.

Un nuovo dominio acquistato da un altro registrar

Quando acquisti un dominio da un altro registrar, ad esempio, poiché il dominio di primo livello (TLD) non è offerto da Route 53, puoi comunque gestire il routing DNS utilizzando Route 53. Per ulteriori informazioni, consulta Domini che è possibile registrare con Amazon Route 53.

Segui queste istruzioni per creare una zona ospitata pubblica e poi usa i name server creati con il registrar:

Per creare una zona ospitata per un dominio diverso da Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione scegli Zone ospitate e quindi Crea zona ospitata.
3. Per il nome, inserisci il nome del dominio per cui desideri creare una zona ospitata, ad esempio una descrizione opzionale`example.com`, scegli Zona ospitata pubblica e quindi Crea zona ospitata.
4. Dopo aver creato la zona ospitata, annota i quattro record del name server (NS) che sono stati creati. Ciascuno inizierà con «ns-».

   Nel registrar del dominio, inserisci i name server indicati in alto per delegare la gestione del dominio alla tua zona ospitata su Route 53.

Instrada il traffico DNS

Per specificare come si desidera che Route 53 instradi il traffico Internet per il dominio, crea i record nella zona ospitata. Ad esempio, se desideri indirizzare le richieste per example.com a un server Web in esecuzione su un' EC2 istanza Amazon, crei un record nella zona ospitata da example.com e specifichi l'indirizzo IP elastico per l'istanza. EC2 Per ulteriori informazioni, consulta i seguenti argomenti:

- Per informazioni su come creare record nella propria zona ospitata, consultare Utilizzo dei record.
- Per informazioni su come indirizzare il traffico verso risorse selezionate AWS , consulta. Instradamento del traffico Internet verso le tue risorse AWS

- Per ulteriori informazioni sul funzionamento di questo DNS, consultare In che modo il traffico Internet viene instradato al tuo sito o applicazione Web.
- Per verificare la reposizione del DNS, consulta. Verifica delle risposte DNS da Route 53

Routing del traffico alle risorse

Quando gli utenti richiedono il tuo sito Web o la tua applicazione Web, ad esempio inserendo il nome del tuo dominio in un browser Web, Amazon Route 53 aiuta a instradare gli utenti alle tue risorse, come un bucket Amazon S3 o un server Web nel tuo data center. Per configurare Route 53 in modo che instradi il traffico verso le tue risorse, completa le seguenti operazioni:

1. Crea una zona ospitata. Puoi creare una zona ospitata pubblica o privata:

   Zona ospitata pubblica

   Crea una zona pubblica ospitata se desideri indirizzare il traffico Internet verso le tue risorse, ad esempio, in modo che i tuoi clienti possano visualizzare il sito Web aziendale che offri su EC2 alcune istanze. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate pubbliche.

   Zona ospitata privata

   Crea una zona ospitata privata se desideri instradare il traffico all'interno di un Amazon VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.
2. Crea record nella zona ospitata. I record definiscono dove desideri instradare il traffico per ciascun nome di dominio o nome di sottodominio. Ad esempio, per instradare il traffico per www.esempio.com a un server Web nel tuo data center, in genere crei un record www.esempio.com nella zona ospitata esempio.com.

   Per ulteriori informazioni, consulta i seguenti argomenti:

   - Utilizzo dei record
   - Routing del traffico per sottodomini
   - Instradamento del traffico Internet verso le tue risorse AWS

Routing del traffico per sottodomini

Quando desideri instradare il traffico verso le risorse per un sottodominio, ad esempio acme.esempio.com o zenith.esempio.com, hai due opzioni:

Creazione di record nella zona ospitata per il dominio

Di solito, per instradare il traffico per un sottodominio, crei un record nella zona ospitata con lo stesso nome del dominio. Ad esempio, per instradare il traffico Internet per acme.esempio.com a un server Web nel data center, crei un record di nome acme.esempio.com nella zona ospitata esempio.com. Per ulteriori informazioni, vedere l'argomento Utilizzo dei record e i relativi sottoargomenti.

Creazione di una zona ospitata per il sottodominio e creazione di record nella nuova zona ospitata

Puoi anche creare una zona ospitata per il sottodominio. L'utilizzo di una zona ospitata separata per instradare il traffico Internet per un sottodominio è anche noto come "delega di responsabilità per un sottodominio a una zona ospitata", "delega di un sottodominio ad altri server dei nomi" o combinazioni simili di termini. Ecco una panoramica di come funziona:

1. Crea una zona ospitata con lo stesso nome del sottodominio di cui desideri instradare il traffico, ad esempio acme.esempio.com.
2. Quindi puoi creare record nella nuova zona ospitata che definiscono il modo in cui desideri instradare il traffico per il sottodominio (acme.esempio.com) e i relativi sottodomini, ad esempio backend.acme.esempio.com.
3. Ottieni i server dei nomi che sono stati assegnati da Route 53 alla nuova zona ospitata al momento della creazione.
4. Crea un nuovo record NS nella zona ospitata per il dominio (example.com) e specifica i quattro server dei nomi ottenuti alla fase 3.

Quando utilizzi una zona ospitata separata per instradare il traffico per un sottodominio, puoi utilizzare le autorizzazioni IAM per limitare l'accesso alla zona ospitata per il sottodominio. Se disponi di sottodomini multipli gestiti da diversi gruppi, la creazione di una zona ospitata per ciascun sottodominio può notevolmente ridurre il numero di persone che devono avere l'accesso ai record nella zona ospitata per quel dominio.

L'utilizzo di una zona ospitata separata per un sottodominio ti consente inoltre di usare servizi DNS diversi per il dominio e il sottodominio. Per ulteriori informazioni, consulta Utilizzo di Amazon Route 53 come servizio DNS per i sottodomini senza migrare il dominio padre.

C'è un piccolo impatto sulle prestazioni su questa configurazione per la prima query DNS da ciascun resolver DNS. Il resolver deve ottenere le informazioni dalla zona ospitata per il dominio radice e quindi ottenere le informazioni dalla zona ospitata per il sottodominio. Dopo la prima query DNS per un sottodominio, il resolver memorizza le informazioni nella cache e non deve

ottenerle di nuovo finché il TTL non scade e un altro client richiede il sottodominio da quel resolver. Per ulteriori informazioni, consulta TTL (secondi) nella sezione Di seguito sono descritti i valori che devi specificare durante la creazione o la modifica di record di Amazon Route 53..

Argomenti

- Creazione di un'altra zona ospitata per instradare il traffico per un sottodominio
- Routing del traffico per ulteriori livelli di sottodomini

Creazione di un'altra zona ospitata per instradare il traffico per un sottodominio

Un modo per instradare il traffico per un sottodominio consiste nel creare una zona ospitata per il sottodominio e quindi creare record per il sottodominio nella nuova zona ospitata. (L'opzione più comune è quella di creare record per il sottodominio nella zona ospitata per il dominio.)

> **Note**
>
> Mentre viene descritto qui il processo per la creazione e la delega a una zona ospitata del sottodominio in Route 53, è anche possibile creare una zona DNS su altri server dei nomi e creare in modo simile record del server dei nomi (NS) che delegano la responsabilità a tali server dei nomi.

Ecco una panoramica del processo:

1. Creare una zona ospitata per il sottodominio. Per ulteriori informazioni, consulta Creazione di una nuova zona ospitata per un sottodominio.
2. Aggiungere record alla zona ospitata per il sottodominio. Se la zona ospitata per il dominio contiene record appartenenti alla zona ospitata per il sottodominio, duplicare quei record nella zona ospitata per il sottodominio. Per ulteriori informazioni, consulta Creazione di record nella zona ospitata per il sottodominio
3. Creare un record NS per il sottodominio nella zona ospitata per il dominio, che delega la responsabilità per il sottodominio al server dei nomi della nuova zona ospitata. Se la zona ospitata per il dominio contiene record appartenenti alla zona ospitata per il sottodominio, eliminare i record dalla zona ospitata per il dominio. (Nel passaggio 2 sono state create copie nella zona ospitata per il sottodominio.) Per ulteriori informazioni, consulta Aggiornamento della zona ospitata per il dominio.

Creazione di una nuova zona ospitata per un sottodominio

Per creare una zona ospitata per un sottodominio utilizzando la console Route 53, esegui la procedura seguente.

Per creare una zona ospitata per un sottodominio (console)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. I nuovi utenti di Route 53 possono consultare Nozioni di base.

   Se stai già utilizzando Route 53, scegli Zone ospitate nel pannello di navigazione.
3. Scegli Crea zona ospitata.
4. Nel riquadro di destra, inserire il nome del sottodominio, ad esempio acme.esempio.com. Facoltativamente, è anche possibile inserire un commento.

   Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.
5. Per Tipo, accetta il valore di default di Zona ospitata pubblica.
6. Nella parte inferiore al riquadro di destra, scegli Crea zona ospitata.

Creazione di record nella zona ospitata per il sottodominio

Per definire il modo in cui desideri che Route 53 instradi il traffico per il sottodominio (acme.esempio.com) e per i suoi sottodomini (backend.acme.esempio.com), crea record nella zona ospitata per il sottodominio.

Tieni presente quanto segue in merito alla creazione di record nella zona ospitata per il sottodominio:

- Non creare ulteriori record di server dei nomi (NS) o di origine di autorità (SOA) nella zona ospitata per il sottodominio e non eliminare i record SOA e NS esistenti.
- Crea tutti i record per il sottodominio nella zona ospitata per il sottodominio. Ad esempio, se disponi di zone ospitate per il dominio esempio.com e apex.esempio.com, crea tutti i record per il sottodominio acme.esempio.com nella zona ospitata di acme.esempio.com. Questo include record come backend.acme.esempio.com e beta.backend.acme.esempio.com.
- Se la zona ospitata per il dominio (esempio.com) contiene già record che appartengono alla zona ospitata per il sottodominio (acme.esempio.com), duplica quei record nella zona ospitata per il

sottodominio. Nell'ultima fase del processo, elimina successivamente i record duplicati della zona ospitata per il dominio.

> **Important**
>
> Se disponi di alcuni record per il sottodominio sia nella zona ospitata per il dominio sia nella zona ospitata per sottodominio, il comportamento di DNS sarà incoerente. Il comportamento dipenderà dai server dei nomi memorizzati nella cache da un resolver DNS, dai server dei nomi per la zona ospitata del dominio (esempio.com) o dai server dei nomi per la zona ospitata del sottodominio (acme.esempio.com). In alcuni casi, Route 53 restituirà NXDOMAIN (dominio inesistente) se il record esiste, ma non nella zona ospitata alla quale il resolver DNS sta inviando la query.

Per ulteriori informazioni, consulta Utilizzo dei record.

Aggiornamento della zona ospitata per il dominio

Quando crei una zona ospitata, Route 53 assegna automaticamente quattro server dei nomi alla zona. Il record NS per una zona ospitata identifica i server dei nomi che rispondono alle query DNS per il dominio o il sottodominio. Per iniziare a utilizzare i record nella zona ospitata per il sottodominio per instradare il traffico Internet, crea un nuovo record NS nella zona ospitata per il dominio (esempio.com) e assegnale il nome del sottodominio (acme.esempio.com). Per il valore del record NS, specifica i nomi dei server dei nomi della zona ospitata per il sottodominio.

Ecco cosa succede quando Route 53 riceve una query DNS da un resolver DNS per il sottodominio acme.esempio.com o uno dei suoi sottodomini:

1. Route 53 esegue una ricerca nella zona ospitata per il dominio (esempio.com) e trova il record NS per il sottodominio (acme.esempio.com).
2. Route 53 ottiene i server dei nomi dal record NS di acme.esempio.com nella zona ospitata per il dominio, esempio.com e restituisce quei server dei nomi al resolver DNS.
3. Il resolver invia di nuovo la query per acme.esempio.com ai server dei nomi per la zona ospitata acme.esempio.com.
4. Route 53 risponde alla query utilizzando un record nella zona ospitata acme.esempio.com.

Per configurare Route 53 affinché instradi il traffico per il sottodominio utilizzando la zona ospitata per il sottodominio e per eliminare eventuali record duplicati della zona ospitata per il dominio, completa la procedura seguente:

Come configurare Route 53 in modo che utilizzi la zona ospitata per il sottodominio (console)

1. Nella console Route 53, ottenere i server dei nomi per la zona ospitata per il sottodominio:
   a. Nel pannello di navigazione, scegli Zone ospitate.
   b. Nella pagina Zone ospitate, scegli il nome per la zona ospitata per il sottodominio.
   c. Nel riquadro a destra, copia i nomi dei quattro server elencati per Server dei nomi nella sezione Dettagli delle zone ospitate.
2. Scegliere il nome della zona ospitata per il dominio (esempio.com), non per il sottodominio.
3. Scegli Crea record.
4. Scegli Routing semplice, quindi scegli Successivo.
5. Scegli Define simple record (Definisci record semplice).
6. Specifica i seguenti valori:

   Nome

   Inserire il nome del sottodominio.

   Valore/instradamento traffico a

   Scegli Indirizzo IP o un altro valore a seconda del tipo di record e incolla i nomi dei server dei nomi copiati nella fase 1.

   Tipo di record

   Sceglie NS - Server di nomi per una zona ospitata.

   TTL (secondi)

   Modificare in un valore più comune per un record NS, ad esempio 172.800 secondi.
7. Scegli Definisci record semplice e scegli Crea record.
8. Se la zona ospitata per il dominio contiene record che sono stati ricreati nella zona ospitata per il sottodominio, eliminare quei record dalla zona ospitata per il dominio. Per ulteriori informazioni, consulta Eliminazione di record.

   Al termine, tutti i record per il sottodominio devono essere nella zona ospitata per il sottodominio.

Routing del traffico per ulteriori livelli di sottodomini

Puoi instradare il traffico a un sottodominio di un sottodominio, come backend.acme.esempio.com, nello stesso modo in cui instradi il traffico a un sottodominio, ad esempio acme.esempio.com. O crei record nella zona ospitata per il dominio, o crei una zona ospitata per il sottodominio di livello inferiore, per poi creare record in quella nuova zona ospitata.

Se scegli di creare una zona ospitata separata per il sottodominio di livello inferiore, crea il record NS per il sottodominio di livello inferiore nella zona ospitata per il sottodominio che si trova più vicino di un livello al nome di dominio. Questo contribuisce a garantire il corretto instradamento del traffico alle tue risorse. Ad esempio, supponi di voler instradare il traffico per i seguenti sottodomini:

- subdomain1.esempio.com
- subdomain2.subdomain1.esempio.com

Per utilizzare un'altra zona ospitata per instradare il traffico per subdomain2.subdomain1.esempio.com, procedi nel seguente modo:

1. Crea una zona ospitata con il nome named subdomain2.subdomain1.esempio.com.
2. Crea record nella zona ospitata subdomain2.subdomain1.esempio.com. Per ulteriori informazioni, consulta Creazione di record nella zona ospitata per il sottodominio.
3. Copia i nomi dei server dei nomi per la zona ospitata subdomain2.subdomain1.esempio.com.
4. Nella zona ospitata subdomain1.esempio.com, crea un record NS di nome subdomain2.subdomain1.esempio.com e incolla i nomi dei server dei nomi per la zona ospitata subdomain2.subdomain1.esempio.com.

   Inoltre, elimina qualsiasi record duplicato di subdomain1.esempio.com. Per ulteriori informazioni, consulta Aggiornamento della zona ospitata per il dominio.

   Dopo aver creato il record NS, Route 53 inizia a usare la zona ospitata subdomain2.subdomain1.esempio.com per instradare il traffico per il sottodominio subdomain2.subdomain1.esempio.com.

Utilizzo delle zone ospitate

Una zona ospitata è un container di record e i record contengono informazioni relative alle modalità con cui desideri instradare il traffico per un dominio specifico (come esempio.com) e i

suoi sottodomini (come acme.esempio.com, zenith.esempio.com). Una zona ospitata e il dominio corrispondente hanno lo stesso nome. Esistono due tipi di zone ospitate:

- Zone ospitate pubbliche contengono record che specificano come instradare il traffico su Internet. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate pubbliche.
- Zone ospitate private contengono record che specificano come instradare il traffico in un VPC Amazon. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.

Utilizzo delle zone ospitate pubbliche

Una zona ospitata pubblica è un container che detiene informazioni relative alle modalità con cui desideri instradare il traffico su Internet per un dominio specifico (come esempio.com) e i suoi sottodomini (come acme.esempio.com, zenith.esempio.com). Puoi ottenere una zona ospitata pubblica in uno dei seguenti modi:

- Quando record il dominio con Route 53 creiamo automaticamente una zona ospitata per tuo conto.
- Quando trasferisci il servizio DNS per un dominio esistente su Route 53, inizi creando una zona ospitata per il dominio. Per ulteriori informazioni, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

In entrambi i casi, crei i record nella zona ospitata per specificare come desideri instradare il traffico per i domini e i sottodomini. Ad esempio, potresti creare un record per indirizzare il traffico di www.example.com verso una CloudFront distribuzione o un server Web nel tuo data center. Per ulteriori informazioni sul record, consulta Utilizzo dei record.

In questo argomento viene descritto come utilizzare la console Amazon Route 53 per creare, elencare ed eliminare zone ospitate pubbliche.

> **Note**
>
> Puoi anche utilizzare una zona ospitata privata Route 53 per indirizzare il traffico all'interno di una o più VPCs zone create con il servizio Amazon VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.

Argomenti

- Considerazioni sull'utilizzo delle zone ospitate pubbliche

- Creazione di una zona ospitata pubblica
- Ottenere i server di nomi per una zona ospitata pubblica
- Elencare le zone ospitate pubbliche
- Visualizzazione dei parametri delle query DNS per una zone ospitata pubblica
- Eliminazione di una zona ospitata pubblica
- Verifica delle risposte DNS da Route 53
- Configurazione dei server di nomi white label
- Record NS e SOA creati da Amazon Route 53 per una zona ospitata pubblica

Considerazioni sull'utilizzo delle zone ospitate pubbliche

Tieni in considerazione le seguenti informazioni quando lavori con zone ospitate pubbliche:

Record NS e SOA

Quando crei una zona ospitata, Amazon Route 53 crea automaticamente un record di server di nomi (NS) e un record di origine di autorità (SOA) per la zona. Il record NS identifica i quattro server di nomi che fornisci al tuo registrar o al servizio DNS in modo che le query DNS vengono instradate ai server dei nomi Route 53. Per ulteriori informazioni sui record NS e SOA, consulta Record NS e SOA creati da Amazon Route 53 per una zona ospitata pubblica.

Più zone ospitate con lo stesso nome

Puoi creare più di una zona ospitata con lo stesso nome e aggiungere record diversi a ciascuna zona. Route 53 assegna quattro server dei nomi a ogni zona ospitata e i server dei nomi sono diversi per ciascuna di esse. Quando aggiorni i record dei server dei nomi del tuo registrar, fai attenzione a utilizzare i server di nomi per la corretta zona ospitata, ovvero quella che contiene i record che desideri siano utilizzati da Route 53 per rispondere alle query per il tuo dominio. Route 53 non restituisce mai valori per i record in altre zone ospitate che hanno lo stesso nome.

Set di deleghe riutilizzabili

Per impostazione predefinita, Route 53 assegna un insieme univoco di quattro server dei nomi (noti collettivamente come set di delega) per ogni zona ospitata creata. Se desideri creare un numero elevato di zona ospitata, puoi creare un set di delega riutilizzabile in modo programmatico. I set di delega riutilizzabili non sono disponibili nella console Route 53. Quindi, potrai creare zone ospitate a livello di codice e assegnare lo stesso set di delega riutilizzabile (ovvero gli stessi quattro server di nomi) a ciascuna zona ospitata.

I set di delega riutilizzabili semplificano la migrazione del servizio DNS a Route 53 perché è possibile impostare il registrar del nome di dominio in modo che siano utilizzati gli stessi quattro server dei nomi per tutti i domini per cui desideri che Route 53 sia il servizio DNS. Per ulteriori informazioni, CreateReusableDelegationSetconsulta Amazon Route 53 API Reference.

Creazione di una zona ospitata pubblica

Una zona ospitata pubblica è un container che detiene informazioni relative alle modalità con cui desideri instradare il traffico su Internet per un dominio specifico (come esempio.com) e i suoi sottodomini (come acme.esempio.com, zenith.esempio.com). Dopo aver creato una zona ospitata, puoi creare i record che specificano come desideri instradare il traffico per i domini e i sottodomini.

> **Important**
>
> È possibile creare una zona ospitata solo per un dominio che si dispone dell'autorizzazione per amministrare. Normalmente, questo significa che sei proprietario del dominio, ma potresti anche sviluppare un'applicazione per il registrant del dominio.

Come creare una zona ospitata pubblica mediante la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Se non hai esperienza con Route 53, scegli Nozioni di base in Gestione DNS.

   Se stai già utilizzando Route 53, scegli Zone ospitate nel pannello di navigazione.
3. Scegli Crea zona ospitata.
4. Nel riquadro Create zona ospitata (Crea zona ospitata), inserisci il nome del dominio su cui desideri instradare il traffico. Facoltativamente, è anche possibile inserire un commento.

   Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.
5. Per Tipo, accetta il valore di default di Public Hosted Zone (Zona ospitata pubblica).
6. Scegli Create (Crea) .
7. Crea record che specificano il modo in cui desideri instradare il traffico per il dominio e i sottodomini. Per ulteriori informazioni, consulta Utilizzo dei record.

8. Per utilizzare i record nella nuova zona ospitata per instradare il traffico per il tuo dominio, consulta l'argomento relativo:

   - Se stai utilizzando Route 53 come servizio DNS per un dominio registrato con un altro registrar di dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.
   - Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

Ottenere i server di nomi per una zona ospitata pubblica

È possibile ottenere i server dei nomi per una zona ospitata pubblica se si desidera modificare il servizio DNS per la registrazione del dominio. Per informazioni su come modificare il servizio DNS, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

> **Note**
>
> Alcuni registrar consentono di specificare i server di nomi solo utilizzando gli indirizzi IP e non consentono di specificare nomi di dominio completi. Se il registrar richiede l'utilizzo di indirizzi IP, puoi ottenere gli indirizzi IP per i tuoi server di nomi utilizzando l'utility dig (per Mac, Unix o Linux) o l'utility nslookup (per Windows). Solo raramente modifichiamo gli indirizzi IP dei server di nomi; se è necessario modificare gli indirizzi IP, ti invieremo una notifica in anticipo.

Come ottenere i server dei nomi per una zona ospitata tramite la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata, quindi seleziona Visualizza dettagli.
4. Nella pagina dei dettagli della zona ospitata, scegli Dettagli della zona ospitata.
5. Prendi nota dei quattro server indicati per Server dei nomi.

Elencare le zone ospitate pubbliche

Puoi utilizzare la console Amazon Route 53 per elencare tutte le zone ospitate che hai creato con l' AWS account corrente. Per informazioni su come elencare le zone ospitate utilizzando l'API Route 53, ListHostedZonesconsulta Amazon Route 53 API Reference.

Per elencare le zone ospitate pubbliche associate a un AWS account utilizzando la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate. La pagina mostra un elenco delle zone ospitate associate all' AWS account con cui hai attualmente effettuato l'accesso.
3. Per filtrare le zone ospitate, utilizza la barra di ricerca situata nella parte superiore della tabella.

   Cerca comportamento varia a seconda che la zona ospitata zone contiene fino a 2.000 record o più di 2.000 record:

   Fino a 2.000 zone ospitate

   - Per visualizzare i record con valori specifici, fai clic sulla barra di ricerca, scegli una proprietà dall'elenco a discesa e immetti un valore. È inoltre possibile immettere un valore direttamente nella barra di ricerca e premere Invio. Ad esempio, per visualizzare le zone ospitate con un nome che inizia con **abc**, immetti quel valore nella barra di ricerca e premi Invio.
   - Per visualizzare solo le zone ospitate con lo stesso tipo di zona ospitata, seleziona il tipo dall'elenco a discesa e immetti il tipo.

   Più di 2.000 zone ospitate

   - È possibile cercare le proprietà in base al nome di dominio esatto, a tutte le proprietà e al tipo.
   - Ricerca utilizzando il nome di dominio esatto per risultati di ricerca più rapidi.

Visualizzazione dei parametri delle query DNS per una zone ospitata pubblica

Puoi visualizzare il numero totale di query DNS a cui Route 53 risponde per una determinata zona ospitata pubblica o una combinazione di zone ospitate pubbliche. Le metriche vengono visualizzate in CloudWatch, il che consente di visualizzare un grafico, scegliere il periodo di tempo che si desidera visualizzare e personalizzare le metriche in molti altri modi. Puoi anche creare allarmi e configurare

notifiche, in modo da ricevere una notifica quando il numero di query DNS in un periodo di tempo specificato supera o scende al di sotto di un livello specificato.

> **Note**
>
> Route 53 invia automaticamente il numero di query DNS a tutte CloudWatch le zone pubbliche ospitate, quindi non è necessario configurare nulla prima di poter visualizzare le metriche delle query. Non sono previsti costi per i parametri delle query DNS.

Quali query DNS vengono conteggiate?

I parametri includono solo le query inoltrate dai resolver DNS a Route 53. Se un resolver DNS ha già memorizzato nella cache la risposta a una query (ad esempio l'indirizzo IP per un load balancer per esempio.com), il resolver continuerà a restituire la risposta memorizzata nella cache senza inoltrare le query a Route 53 finché il TTL per il record corrispondente non scade.

In base al numero di query DNS inviate per un nome di dominio (esempio.com) o di sottodominio (www.esempio.com), che gli utenti usano, e in base al TTL per il record, i parametri delle query DNS potrebbero contenere informazioni su una sola query rispetto a diverse migliaia di query che vengono inviate ai resolver DNS. Per ulteriori informazioni sul funzionamento di DNS, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Quando iniziano a comparire in CloudWatch i parametri di query per una zona ospitata?

Dopo aver creato una zona ospitata, possono passare diverse ore prima che la zona ospitata possa comparire in CloudWatch. Inoltre, è necessario inviare una query DNS per un record nella zona ospitata affinché ci siano dati da visualizzare.

I parametri sono disponibili solo negli Stati Uniti orientali (Virginia settentrionale)

Per ottenere i parametri nella console, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione. Per ottenere le metriche utilizzando la AWS CLI, devi lasciare AWS la Regione non specificata o `us-east-1` specificarla come Regione. Se scegli qualsiasi altra regione, i parametri di Route 53 non saranno disponibili.

CloudWatch metrica e dimensione per le query DNS

Per informazioni sulla CloudWatch metrica e sulla dimensione per le query DNS, consulta. Monitoraggio delle zone ospitate tramite Amazon CloudWatch Per informazioni sui CloudWatch parametri, consulta Using Amazon CloudWatch metrics nella Amazon CloudWatch User Guide.

Ottenere più dati dettagliati relativi alle query DNS

Per ottenere informazioni più dettagliate su ogni query DNS a cui Route 53 risponde, inclusi i seguenti riportati di seguito, puoi configurare la registrazione delle query:

- Dominio o sottodominio richiesto
- Data e ora della richiesta
- Tipo di record DNS (ad esempio A o AAAA)
- Edge location Route 53 che ha risposto alla query DNS
- Codice di risposta DNS, ad esempio `NoError` o `ServFail`

Per ulteriori informazioni, consulta Registrazione delle query DNS pubbliche.

Come ottenere parametri delle query DNS

Poco dopo aver creato una zona ospitata, Amazon Route 53 inizia a inviare metriche e dimensioni una volta al minuto a CloudWatch. Puoi utilizzare le seguenti procedure per visualizzare i parametri sulla CloudWatch console o visualizzarli utilizzando AWS Command Line Interface ()AWS CLI.

Argomenti

- Visualizzazione delle metriche delle query DNS per una zona ospitata pubblica nella console CloudWatch
- Ottenere le metriche delle query DNS utilizzando AWS CLI

Visualizzazione delle metriche delle query DNS per una zona ospitata pubblica nella console CloudWatch

Per visualizzare i parametri delle query DNS per le zone ospitate pubbliche nella CloudWatch console, eseguire la procedura seguente.

Per visualizzare i parametri delle query DNS per una zona ospitata pubblica sulla console CloudWatch

1. Accedi a AWS Management Console e apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nel riquadro di navigazione, seleziona Parametri.

3. Nell'elenco delle AWS regioni nell'angolo superiore destro della console, scegli Stati Uniti orientali (Virginia settentrionale). Le metriche di Route 53 non sono disponibili se scegli un'altra AWS regione.
4. Nella scheda All metrics (Tutti i parametri) scegliere Route 53.
5. Scegli Hosted Zone Metrics (Parametri zona ospitata).
6. Seleziona la casella di controllo per una o più zone ospitate con il nome della metrica. DNSQueries
7. Nella scheda Graphed metrics (Parametri definiti), modifica i valori applicabili per visualizzare i parametri nel formato desiderato.

   Per Statistica, scegli Somma o SampleCount; entrambe le statistiche mostrano lo stesso valore.

Ottenere le metriche delle query DNS utilizzando AWS CLI

Per ottenere le metriche delle query DNS utilizzando il AWS CLI, si utilizza il comando. get-metric-data Tieni presente quanto segue:

- Specifica la maggior parte dei valori per il comando in un file JSON separato. Per ulteriori informazioni, consulta get-metric-data.
- Il comando restituisce un valore per ogni intervallo specificato per `Period` nel file JSON. `Period` è espresso in secondi, pertanto se specifichi un periodo di tempo di cinque minuti e specifichi `60` per `Period`, otterrai cinque valori. Se specifichi un periodo di tempo di cinque minuti e specifichi `300` per `Period`, otterrai un valore.
- Nel file JSON, puoi specificare qualsiasi valore per `Id`.
- Lasciate la AWS regione non specificata o specificatela `us-east-1` come regione. Se scegli qualsiasi altra regione, i parametri di Route 53 non saranno disponibili. Per ulteriori informazioni, consulta Configurazione della AWS CLI nella Guida per AWS Command Line Interface l'utente.

Ecco il AWS CLI comando che usi per ottenere i parametri delle query DNS per il periodo di cinque minuti compreso tra le 4:01 e le 4:07 del 1° maggio 2019. Il parametro `metric-data-queries` fa riferimento al file JSON di esempio che segue il comando.

```
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
```

Di seguito è riportato il file JSON di esempio:

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

Di seguito è riportato l'output di questo comando. Tieni presente quanto segue:

- L'ora di inizio e l'ora di fine nel comando coprono un periodo di tempo di sette minuti, da `2019-05-01T04:01:00Z` a `2019-05-01T04:07:00Z`.
- I valori restituiti sono solo sei. Non esiste alcun valore per `2019-05-01T04:05:00Z` perché durante quel minuto non ci sono state query DNS.
- Il valore di `Period` specificato nel file JSON è `60` (secondi), pertanto i valori vengono segnalati a intervalli di un minuto.

```
{
    "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"
            ]
        }
    ]
}
```

Eliminazione di una zona ospitata pubblica

Questa sezione illustra come eliminare una zona ospitata pubblica utilizzando la console Amazon Route 53.

Puoi eliminare una zona ospitata solo se non sono presenti record diversi dai record SOA e NS di default. Se la tua zona ospitata contiene altri record, devi eliminarli prima di eliminare la zona ospitata. In questo modo si impedisce l'eliminazione accidentale di una zona ospitata che contiene ancora record.

Argomenti

- Impedire che il traffico venga instradato al dominio
- Eliminazione di zone ospitate pubbliche create da un altro servizio
- Utilizzo della console Route 53 per eliminare una zona ospitata pubblica

Impedire che il traffico venga instradato al dominio

Se desideri mantenere la registrazione del tuo dominio, ma desideri interrompere il routing del traffico Internet sul tuo sito o applicazione Web, ti consigliamo di eliminare i record nella zona ospitata invece di eliminarla.

> **Important**
>
> Se elimini una zona ospitata, non puoi annullarne l'eliminazione. Devi creare una nuova zona ospitata e aggiornare i server di nomi per la registrazione del tuo dominio, operazione che può richiedere fino a 48 ore per rendere effettiva la modifica. Inoltre, se elimini una zona ospitata, qualcuno potrebbe dirottare il dominio e instradare il traffico verso le proprie risorse utilizzando il tuo nome di dominio.
>
> Se è stata delegata la responsabilità di un sottodominio a una zona ospitata e si desidera eliminare la zona ospitata figlio, è inoltre necessario aggiornare la zona ospitata padre eliminando il record NS con lo stesso nome della zona ospitata figlio. Ad esempio, se si desidera eliminare la zona ospitata acme.example.com, è necessario eliminare anche il record NS acme.example.com nella zona ospitata example.com. Prima di eliminare la zona ospitata figlio, si consiglia di eliminare il record NS e di attendere la durata del TTL del record NS. Ciò impedisce il dirottamento della zona ospitata figlio per il periodo di tempo in cui i resolver DNS includono ancora nella cache i server dei nomi per la zona ospitata figlio.

Se desideri evitare di pagare la tariffa mensile per la zona ospitata, puoi trasferire il servizio DNS per il dominio a un servizio DNS gratuito. Quando trasferisci un servizio DNS, è necessario aggiornare i server di nomi per la registrazione del dominio. Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio per informazioni su come sostituire i server dei nomi di Route 53 con i server di nomi per il nuovo servizio DNS. Se il dominio è registrato con un altro registrar, utilizza il metodo fornito dal registrar per aggiornare i server di nomi per la registrazione del dominio. Per ulteriori informazioni, esegui una ricerca su Internet immettendo la query "servizio DNS gratuito".

Eliminazione di zone ospitate pubbliche create da un altro servizio

Se una zona ospitata è stata creata da un altro servizio, non sarà possibile eliminarla utilizzando la console Route 53. Al contrario, è necessario utilizzare il processo applicabile all'altro servizio:

- AWS Cloud Map— Per eliminare una zona ospitata AWS Cloud Map creata quando hai creato uno spazio dei nomi DNS pubblico, elimina lo spazio dei nomi. AWS Cloud Map elimina automaticamente la zona ospitata. Per ulteriori informazioni, consulta Eliminazione degli spazi dei nomi nella Guida per gli sviluppatori di AWS Cloud Map .
- Rilevamento del servizio Amazon Elastic Container Service (Amazon ECS): per eliminare una zona ospitata pubblica creata da Amazon ECS quando hai creato un servizio utilizzando l'individuazione dei servizi, eliminare i servizi Amazon ECS che utilizzano lo spazio dei nomi ed eliminare lo

spazio dei nomi. Per ulteriori informazioni, consulta Eliminazione di un servizio nella Guida per gli sviluppatori di Amazon Elastic Container Service.

Utilizzo della console Route 53 per eliminare una zona ospitata pubblica

Per utilizzare la console Route 53 per eliminare una zona ospitata pubblica, completa la procedura seguente.

Come eliminare una zona ospitata pubblica tramite la console Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Hosted zones (Zone ospitate) e scegli il link evidenziato per la zona ospitata che desideri eliminare.
3. Conferma che la zona ospitata che desideri eliminare contiene solo un record NS e un record SOA. Se contiene registri aggiuntivi, eliminali. Sarà inoltre necessario disabilitare la firma DNSSEC:

   - Nella pagina dei dettagli della zona ospitata, nell'elenco Records (Registri), se l'elenco dei record include i record per i quali il valore della colonna Type (Tipo) è diverso da NS o SOA, scegli la riga, quindi seleziona Delete (Elimina).

     Per selezionare più record consecutivi, seleziona la prima riga, tieni premuto il tasto Shift (MAIUSC) e seleziona l'ultima riga. Per selezionare più record non consecutivi, seleziona la prima riga, tieni premuto il tasto Ctrl e seleziona le righe rimanenti.

     > **Note**
     >
     > Se hai creato record NS per sottodomini nella hosted zone, elimina anche questi record.

4. Torna alla pagina Hosted zones (Zone ospitate) e scegli la riga per la zona ospitata che desideri eliminare.
5. Scegli Elimina.
6. Digita la chiave di conferma e scegli Elimina.

7. Se desideri rendere il dominio non disponibile su Internet, ti consigliamo di trasferire il servizio DNS su un servizio DNS gratuito e quindi eliminare la zona ospitata di Route 53. In questo modo si impedisce che query DNS future vengano instradate in modo non corretto.

   Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio per informazioni su come sostituire i server dei nomi di Route 53 con i server di nomi per il nuovo servizio DNS. Se il dominio è registrato con un altro registrar, utilizza il metodo fornito dal registrar per modificare i server di nomi per il dominio.

   > **Note**
   >
   > Se stai eliminando una zona ospitata per un sottodominio (acme.esempio.com), non è necessario modificare i server di nomi per il dominio (esempio.com).

Verifica delle risposte DNS da Route 53

Se hai creato una zona ospitata di Amazon Route 53 per il tuo dominio, puoi utilizzare lo strumento di controllo DNS nella console per vedere in che modo Route 53 risponderà alle query DNS se configuri il dominio per utilizzare Route 53 come servizio DNS. Per i record di geolocalizzazione, geoprossimità e latenza, puoi anche simulare le query da un determinato resolver DNS e/o indirizzo IP client per scoprire quale risposta Route 53 restituirebbe.

> **Important**
>
> Lo strumento non invia query al Domain Name System, ma risponde solo in base alle impostazioni nei record nella zona ospitata. Lo strumento restituisce le stesse informazioni indipendentemente dal fatto che la zona ospitata sia attualmente utilizzata per instradare il traffico per il dominio.

Lo strumento di controllo DNS funziona solo per zone ospitate pubbliche.

> **Note**
>
> Lo strumento di controllo DNS restituisce informazioni simili a quelle solitamente fornite dalla sezione di risposta del comando `dig`. Pertanto, se esegui una query per i server di nomi di un sottodominio che puntano ai server di nomi padre, questi non verranno restituiti.

Argomenti

Utilizzo dello strumento di controllo per vedere come Amazon Route 53 risponde alle query DNS

Puoi utilizzare lo strumento per vedere le risposte restituite da Amazon Route 53 in risposta a una query DNS per un record.

Come utilizzare lo strumento di controllo per vedere come Route 53 risponde alle query DNS

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate).
3. Nella pagina Hosted zones (Zone ospitate) , scegli il nome di una zona ospitata. La console visualizza l'elenco dei record per tale hosted zone.
4. Per passare direttamente alla pagina Controlla risposta da Route 53, seleziona Test record.
5. Specifica i seguenti valori:
   - Il nome del record, escluso il nome della zona ospitata. Ad esempio, per controllare www.example.com, inserire www. Per controllare example.com, lasciare vuoto il campo Record name (Nome record) .
   - Il tipo di record che si desidera controllare, ad esempio A o CNAME.
6. Scegli Get Response (Ottieni risposta).
7. La sezione Response returned by Route 53 (Risposta restituita da Route 53) include i seguenti valori:

   Codice di risposta DNS

   Un codice che indica se la query era valida o meno. Il codice di risposta più comune è NOERROR, che indica che la query era valida. Se la risposta non è valida, Route 53 restituisce un codice di risposta che spiega il motivo. Per un elenco dei codici di risposta possibili, consulta DNS RCODES sul sito Web di IANA.

   Protocollo

   Il protocollo che è stato usato da Amazon Route 53 per rispondere alla query, UDP o TCP.

Risposta restituita da Route 53

Il valore che Route 53 restituirebbe a un'applicazione Web. Il valore è uno dei seguenti:

- Per i record non di alias, la risposta contiene il valore o i valori nel record.
- Per più record con lo stesso nome e tipo, tra cui record ponderati, di latenza, di geolocalizzazione e di failover, la risposta contiene il valore proveniente dal record appropriato, in base alla richiesta.
- Per i record di alias che si riferiscono a AWS risorse diverse da un altro record, la risposta contiene un indirizzo IP o un nome di dominio per la AWS risorsa, a seconda del tipo di risorsa.
- Per i record alias che fanno riferimento ad altri record, la risposta contiene il valore o i valori provenienti dal record di riferimento.

Utilizzo dello strumento di controllo per la simulazione di query da indirizzi IP specifici (solo record di geolocalizzazione e latenza)

Se hai creato record di latenza o record di geolocalizzazione, puoi utilizzare lo strumento di controllo per simulare le query tramite l'indirizzo IP per un resolver DNS e un client.

Utilizzare lo strumento di controllo per simulare le query da parte di indirizzi IP specificati

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate).
3. Nella pagina Hosted zones (Zone ospitate) , scegli il nome di una zona ospitata. La console visualizza l'elenco dei record per tale hosted zone.
4. Per passare direttamente alla pagina Check response from Route 53 (Controlla riposta da Route 53), seleziona Test record set (Testa serie di record).

   Per passare alla pagina Check response from Route 53 (Controlla riposta da Route 53) per un record specifico, seleziona la casella di controllo per il record e seleziona Test record set (Testa serie di record).
5. Se si è selezionato Test record set (Testa serie di record) senza aver prima scelto un record, specificare i seguenti valori:

- Il nome del record, escluso il nome della zona ospitata. Ad esempio, per controllare www.example.com, inserire www. Per controllare example.com, lasciare vuoto il campo Record name (Nome record) .
- Il tipo di record che si desidera controllare, ad esempio A o CNAME.

6. Specifica i valori applicabili:

   Indirizzo IP del resolver

   Specificate un IPv6 indirizzo IPv4 or per simulare la posizione del resolver DNS utilizzato da un client per effettuare richieste. Questa funzione è utile per il testing dei record di latenza e di geolocalizzazione. Se si omette questo valore, lo strumento utilizza l'indirizzo IP di un resolver DNS nella regione AWS Stati Uniti orientali (Virginia settentrionale) (us-east-1).

   IP sottorete client EDNS0

   Se il resolver supporta EDNS0, digita l'IP della sottorete client per un indirizzo IP nell'ubicazione geografica applicabile, ad esempio, 192.0.2.0 o 2001:db8:85a3::8a2e:370:7334.

   Maschera sottorete

   Se specifichi un indirizzo IP per EDNS0 client subnet IP (IP sottorete client EDNS0) puoi specificare il numero di bit dell'indirizzo IP che desideri che lo strumento di controllo includa nella query DNS. Ad esempio, se specifichi 192.0.2.44 per EDNS0 client subnet IP (IP sottorete client EDNS0) e 24 per Subnet mask (Maschera sottorete), lo strumento di controllo simula una query da 192.0.2.0/24. Il valore predefinito è 24 bit per gli indirizzi e 64 bit per gli indirizzi. IPv4 IPv6

7. Scegli Get Response (Ottieni risposta).
8. La sezione Response returned by Route 53 (Risposta restituita da Route 53) include i seguenti valori:

   Query DNS inviata a Route 53

   La query, in formato BIND, che lo strumento di controllo ha inviato a Route 53. Questo è lo stesso formato che un'applicazione Web utilizzerebbe per inviare una query. I tre valori sono tipicamente il nome del record, IN (per internet), e il tipo di record.

Codice di risposta DNS

Un codice che indica se la query era valida o meno. Il codice di risposta più comune è NOERROR, che indica che la query era valida. Se la risposta non è valida, Route 53 restituisce un codice di risposta che spiega il motivo. Per un elenco dei codici di risposta possibili, consulta DNS RCODES sul sito Web di IANA.

Protocollo

Il protocollo che è stato usato da Amazon Route 53 per rispondere alla query, UDP o TCP.

Risposta restituita da Route 53

Il valore che Route 53 restituirebbe a un'applicazione Web. Il valore è uno dei seguenti:

- Per i record non di alias, la risposta contiene il valore o i valori nel record.
- Per più record con lo stesso nome e tipo, tra cui record ponderati, di latenza, di geolocalizzazione e di failover, la risposta contiene il valore proveniente dal record appropriato, in base alla richiesta.
- Per i record di alias che si riferiscono a AWS risorse diverse da un altro record, la risposta contiene un indirizzo IP o un nome di dominio per la AWS risorsa, a seconda del tipo di risorsa.
- Per i record alias che fanno riferimento ad altri record, la risposta contiene il valore o i valori provenienti dal record di riferimento.

Configurazione dei server di nomi white label

Ogni zona ospitata di Amazon Route 53 è associata a quattro server di nomi, noti collettivamente come set di delega. Per impostazione predefinita, i server di nomi hanno nomi come ns-2048.awsdns-64.com. Se desideri che il nome di dominio del tuo server di nomi sia lo stesso nome di dominio della tua zona ospitata, ad esempio, ns1.esempio.com, puoi configurare nomi di server white label, noti anche come server di nomi vanity o privati.

La procedura seguente spiega come configurare un set di quattro server di nomi white label che puoi riutilizzare per più domini. Ad esempio, supponiamo che possiedi i domini esempio.com, esempio.org ed esempio.net. Grazie a questi passaggi, puoi configurare server di nomi white label per esempio.com e riutilizzarli per esempio.org ed esempio.net.

Argomenti

- Fase 1: Creazione un set di delega Route 53 riutilizzabile

- Fase 2: Creazione o nuova creazione di una zona ospitata di Amazon Route 53 e modifica del TTL per i record NS e SOA
- Fase 3: ricrea record per le hosted zone
- Fase 4: ottenere gli indirizzi IP
- Fase 5: crea record per server di nomi white label
- Fase 6: aggiorna i record NS e SOA
- Fase 7: crea record associati e modifica i server di nomi del registrar
- Fase 8: monitora il traffico per il tuo sito Web o applicazione
- Fase 9: TTLs Tornate ai valori originali
- Fase 10: (opzionale) contatta i servizi DNS ricorsivi

Fase 1: Creazione un set di delega Route 53 riutilizzabile

I server dei nomi con white label sono associati a un set di delega Route 53 riutilizzabile. È possibile utilizzare server di nomi con etichetta bianca per una zona ospitata solo se la zona ospitata e il set di deleghe riutilizzabile sono stati creati dallo stesso account. AWS

Per creare un set di deleghe riutilizzabile, puoi utilizzare l'API Route 53, la AWS CLI o una delle. AWS SDKs Per ulteriori informazioni, consulta la seguente documentazione :

- API Route 53: consulta la CreateReusableDelegationSetguida di riferimento all'API Amazon Route 53
- AWS CLI — Vedi create-reusable-delegation-setnel riferimento ai comandi AWS CLI
- AWS SDKsConsulta la documentazione SDK applicabile nella pagina Documentazione AWS

Fase 2: Creazione o nuova creazione di una zona ospitata di Amazon Route 53 e modifica del TTL per i record NS e SOA

Crea o crea nuovamente le zone ospitate per Amazon Route 53:

- Se non stai utilizzando Route 53 come servizio DNS per i domini per i quali desideri utilizzare server di nomi white label: crea le zone ospitate e specifica il set di delega riutilizzabile creato nella fase precedente con ogni zona ospitata. Per ulteriori informazioni, CreateHostedZoneconsulta Amazon Route 53 API Reference.

- Se stai utilizzando Route 53 come servizio DNS per i domini per i quali desideri utilizzare server di nomi white label: devi creare le zone ospitate per cui desideri utilizzare i server dei nomi white label e specificare il set di delega riutilizzabile creato nella fase precedente per ogni zona ospitata.

> **Important**
>
> Non puoi modificare i server di nomi che sono associati a una zona ospitata esistente. Puoi associare un set di delega riutilizzabile a una zona ospitata solo quando crei la hosted zone.

Quando crei le zone ospitate e prima di tentare di accedere alle risorse per i domini corrispondenti, modifica i seguenti valori di TTL per ogni hosted zone:

- Cambia il valore TTL per il record NS per le zone ospitate su 60 secondi o meno.
- Cambia il valore TTL minimo per il record SOA per le zone ospitate su 60 secondi o meno. Questo è l'ultimo valore nel record SOA.

Se accidentalmente dai al tuo registrar indirizzi IP sbagliati per i server di nomi white label, il tuo sito Web non sarà disponibile e non sarà disponibile per la durata del TTL dopo aver corretto il problema. Impostando un valore TTL basso, puoi ridurre la quantità di tempo per cui il tuo sito Web non è disponibile.

Per ulteriori informazioni sulla creazione di zone ospitate e sulla specifica di un set di delega riutilizzabile per i name server per le zone ospitate, consulta CreateHostedZoneAmazon Route 53 API Reference.

Fase 3: ricrea record per le hosted zone

Crea record nelle zone ospitate create nella fase 2:

- Se stai eseguendo la migrazione del servizio DNS per i tuoi domini ad Amazon Route 53 - potresti essere in grado di creare record importando le informazioni sui record esistenti. Per ulteriori informazioni, consulta Creazione di record mediante importazione di un file di zona.
- Se stai sostituendo le zone ospitate esistenti in modo che sia possibile utilizzare server dei nomi white label: nelle nuove zone ospitate, crea nuovamente i record che appaiono nelle tue zone ospitate correnti. Route 53 non fornisce un metodo per l'esportazione di record da una zona ospitata, ma alcuni fornitori di terze parti lo fanno. Puoi quindi utilizzare la funzione di importazione

di Route 53 per importare record non alias per i quali la policy di routing è semplice. Non vi è alcun modo per esportare e importare nuovamente record o record alias per cui la policy di routing non è semplice.

Per informazioni sulla creazione di record utilizzando l'API Route 53, consulta CreateHostedZoneAmazon Route 53 API Reference. Per informazioni sulla creazione di record utilizzando la console Route 53, consulta Utilizzo dei record.

Fase 4: ottenere gli indirizzi IP

Ottieni gli IPv6 indirizzi IPv4 e gli indirizzi dei name server nel set di delega riutilizzabile e compila la tabella seguente.

Nome di un server di nomi nel set di delega riutilizzabile (ad esempio: ns-2048.awsdns-64.com)	IPv4 e indirizzi IPv6	Nome che desideri assegnare al server di nomi white label (ad esempio: ns1.esempio.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

Ad esempio, supponiamo che i quattro nomi di server per il set di delega riutilizzabile sono:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org

- ns-2051.awsdns-67.co.uk

Di seguito sono descritti i comandi di Linux e Windows da eseguire per ottenere gli indirizzi IP per il primo dei quattro server di nomi:

comandi dig per 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
```

comando nslookup per 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
```

Fase 5: crea record per server di nomi white label

Nella zona ospitata che ha lo stesso nome (ad esempio esempio.com) del nome di dominio del server di nomi white label (ad esempio ns1.esempio.com), crea otto record:

- Un record A per ogni server di nomi white label
- Un record AAAA per ogni server di nomi white label

> **Important**
>
> Se utilizzi gli stessi server di nomi white label per due o più zone ospitate, non eseguire questa operazione per le altre zone ospitate.

Per ogni record, specifica i seguenti valori. Per ulteriori informazioni, consulta la tabella compilata nella fase precedente:

Policy di routing

Specifica Routing semplice.

Nome record

Il nome che desideri assegnare a uno dei tuoi server di nomi white label, ad esempio: ns1.esempio.com. Per il prefisso (ns1 in questo esempio), puoi utilizzare qualsiasi valore valido in un nome di dominio.

Valore/instradamento traffico a

L' IPv6 indirizzo IPv4 o di uno dei name server di Route 53 nel set di delega riutilizzabile.

> **Important**
>
> Se specifichi indirizzi IP sbagliati al momento della creazione di record per i server di nomi white label, il tuo sito o applicazione Web non sarà disponibile su Internet quando esegui le fasi successive. Anche se correggi gli indirizzi IP immediatamente, il tuo sito o applicazione Web rimarrà non disponibile per la durata del TTL.

Tipo di record

Specificare A quando si creano record per gli IPv4 indirizzi.

Specificate AAAA quando create i record per gli IPv6 indirizzi.

TTL (secondi)

Questo valore è la quantità di tempo per cui i resolver DNS memorizzano nella cache le informazioni di questo record prima di inoltrare un'altra query DNS a Route 53. È consigliabile specificare un valore iniziale di 60 secondi o meno, in modo che sia possibile recuperare in modo rapido se accidentalmente si specificano valori errati in questi record.

Fase 6: aggiorna i record NS e SOA

Aggiorna i record SOA e NS nelle zone ospitate per cui desideri utilizzare i server di nomi white label. Esegui le fasi dalla 6 alla 8 per una zona ospitata e il dominio corrispondente alla volta, quindi ripeti la procedura per un'altra zona ospitata e dominio.

> **Important**
>
> Inizia con la zona ospitata di Amazon Route 53 che ha lo stesso nome di dominio (ad esempio esempio.com) del server dei nomi white label (ad esempio ns1.esempio.com).

1. Aggiornamento del record SOA sostituendo il nome del server dei nomi di Route 53 con il nome di uno dei server dei nomi white label

   Esempio

   Sostituisci il nome del server di nomi Route 53:

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   con il nome di uno dei tuoi server di nomi white label:

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > È stato modificato l'ultimo valore, il time to live (TTL) in Fase 2: Creazione o nuova creazione di una zona ospitata di Amazon Route 53 e modifica del TTL per i record NS e SOA.

   Per informazioni sull'aggiornamento di record utilizzando la console Route 53, consulta Modifica di record.
2. Nel record NS, annota i nomi dei server di nomi attuali per il dominio, in modo da poterli ripristinare, se necessario.
3. Aggiorna il record NS. Sostituisci il nome dei server di nomi Route 53 con i nomi dei tuoi quattro server di nomi white label, ad esempio, `ns1.example.com`, `ns2.example.com`, `ns3.example.com` e `ns4.example.com`.

Fase 7: crea record associati e modifica i server di nomi del registrar

Utilizza il metodo fornito dal registrar per creare record associati e modificare i server di nomi del registrar:

1. Aggiungere record associati:

   - Se stai aggiornando il dominio con lo stesso nome di dominio dei server dei nomi white label: crea quattro Glue Record associati per i quali i nomi e gli indirizzi IP corrispondono ai valori che hai ottenuto nella fase 4. Includi IPv4 sia l'indirizzo che l' IPv6 indirizzo di un name server con etichetta bianca nel record Glue corrispondente, ad esempio:

     ns1.example.com: indirizzi IP = 192.0.2.117 e 2001:db8:85a3::8a2e:370:7334

     I registrar utilizzano una serie di termini diversi per i record associati. Questa operazione è nota anche come registrazione di nuovi server di nomi o qualcosa di simile.
   - Se stai aggiornando un altro dominio— Se Route 53 è il servizio DNS, è necessario prima completare il passaggio nel punto precedente e creare i record di colla corrispondenti al nome di dominio. Passare quindi alla fase 2 in questa procedura.
2. Cambia server dei nomi per il dominio con i nomi dei tuoi server di nomi white label.

Se stai utilizzando Amazon Route 53 come servizio DNS, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

Fase 8: monitora il traffico per il tuo sito Web o applicazione

Monitora il traffico per il sito Web o l'applicazione per cui hai creato record associati e modificato i server di nomi nella fase 7:

- Se il traffico si interrompe: utilizza il metodo fornito dal registrar per modificare i server dei nomi per il dominio e riportarli ai precedenti server di nomi di Route 53. Questi sono i server di nomi che avevi annotato nella fase 6b. Stabilisci quindi ciò che non ha funzionato.
- Se il traffico non è influenzato: ripeti le fasi da 6 a 8 per il resto delle zone ospitate per cui desideri utilizzare gli stessi server dei nomi white label.

Fase 9: TTLs Tornate ai valori originali

Per tutte le zone ospitate che ora utilizzano i server di nomi white label, modifica i seguenti valori:

- Cambia il valore TTL per il record NS per le zone ospitate con un valore più tipico per i record NS, per esempio, 172800 secondi (due giorni).
- Cambia il valore TTL minimo per il record SOA per le zone ospitate con un valore più tipico per i record SOA, per esempio, 900 secondi, Questo è l'ultimo valore nel record SOA.

Fase 10: (opzionale) contatta i servizi DNS ricorsivi

Facoltativo Se utilizzi il routing di geolocalizzazione di Amazon Route 53, contatta i servizi DNS ricorsivi che supportano l' edns-client-subnetestensione di EDNS0 e fornisci loro i nomi dei tuoi name server con etichetta bianca. In questo modo questi servizi DNS continueranno a instradare le query DNS alla posizione Route 53 ottimale in base alla posizione geografica approssimativa da cui è provenuta la query.

Record NS e SOA creati da Amazon Route 53 per una zona ospitata pubblica

Per ciascuna zona ospitata creata, Amazon Route 53 crea automaticamente un record di server dei nomi (NS) e un record di origine di autorità (SOA). Raramente è necessario modificare questi record.

Argomenti

Il record di server dei nomi (NS)

Amazon Route 53 crea automaticamente un record di server dei nomi (NS) che ha lo stesso nome della tua zona ospitata. Vengono elencati i quattro server di nomi che sono i server di nomi ufficiali per la tua hosted zone. Tranne che in circostanze rare, si consiglia di non aggiungere, modificare o eliminare i server dei nomi in questo record.

I seguenti esempi mostrano il formato per i nomi di server dei nomi di Route 53 (sono solo esempi; non utilizzarli durante l'aggiornamento dei record di server dei nomi del tuo registrar):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Per ottenere l'elenco dei server di nomi per la tua hosted zone:

1. Accedi e apri la console Route 53 all'indirizzo. AWS Management Console https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.

3. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata, quindi seleziona Visualizza dettagli.
4. Nella pagina dei dettagli della zona ospitata, scegli Dettagli della zona ospitata.
5. Prendi nota dei quattro server indicati per Server dei nomi.

Per ulteriori informazioni sulla migrazione del servizio DNS da un altro provider di servizi DNS a Route 53, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Il record di origine di autorità (SOA)

I; record origine di autorità (SOA) identifica le informazioni DNS di base che interessano il dominio, ad esempio:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Un record SOA include i seguenti elementi:

- Il server dei nomi di Route 53 che ha creato il record SOA, ad esempio, `ns-2048.awsdns-64.net`.
- L'indirizzo e-mail dell'amministratore. Il simbolo `@` è sostituito da un punto, ad esempio `hostmaster.example.com`. Il valore di default è un indirizzo e-mail amazon.com che non è monitorato.
- Un numero di serie che puoi incrementare ogni volta che aggiorni un record nella zona ospitata. Route 53 non incrementa automaticamente il numero. (Il numero di serie viene utilizzato dai servizi DNS che supportano il DNS secondario.) In questo esempio, il valore è `1`.
- Un tempo di aggiornamento in secondi che i server DNS secondari attendono prima di eseguire query sui record SOA dei server DNS primari per verificare la presenza di modifiche. In questo esempio, il valore è `7200`.
- L'intervallo in secondi che un server secondario attende prima di provare il trasferimento di una zona non riuscito. Di solito, il tempo per il nuovo tentativo è inferiore al tempo di aggiornamento. In questo esempio, il valore è `900` (15 minuti).
- Il tempo in secondi per cui un server secondario continuerà a tentare di completare un trasferimento di zona. Se questo trascorre prima del trasferimento, il server secondario smetterà di rispondere alle query perché considera i suoi dati troppo vecchi per essere affidabili. In questo esempio, il valore è `1209600` (due settimane).

- Il TTL minimo. Questo valore consente di definire il periodo di tempo in cui i resolver ricorsivi devono memorizzare nella cache le seguenti risposte da Route 53:

  NXDOMAIN

  Non vi è alcun record di alcun tipo con il nome specificato nella query DNS, ad esempio example.com. Non sono inoltre presenti record figlio del nome specificato nella query DNS, ad esempio zenith.example.com.

  NODATA

  Esiste almeno un record con il nome specificato nella query DNS, ma nessuno di questi record ha il tipo (ad esempio A) specificato nella query DNS.

  Quando un resolver DNS memorizza nella cache un risultato NXDOMAIN, questa operazione viene definita come memorizzazione negativa nella cache.

  La durata della memorizzazione negativa nella cache è il minore dei seguenti valori:

  - Questo valore: il TTL minimo nel record SOA. Nell'esempio, il valore è `86400` (un giorno).
  - Il valore del TTL per il record SOA. Il valore predefinito è 900 secondi. Per informazioni su come modificare questo valore, consulta Modifica di record.

  Quando Route 53 risponde alle query DNS con una risposta NXDOMAIN o NODATA (una risposta negativa), viene addebitata la tariffa per le query standard. Consulta "Query" in Prezzi di Amazon Route 53. Se sei preoccupato per il costo delle risposte negative, un'opzione consiste nel modificare il TTL per il record SOA, il valore TTL minimo nel record SOA (questo valore) o entrambi. Tieni presente che l'aumento di questi valori TTLs, che si applicano alle risposte negative per l'intera zona ospitata, può avere effetti sia positivi che negativi:

  - I resolver DNS di Internet memorizzano nella cache l'inesistenza di record per periodi più lunghi, cosa che riduce il numero di query che vengono inoltrate a Route 53. In questo modo si riduce l'addebito di Route 53 per le query DNS.
  - Tuttavia, se si elimina erroneamente un record valido e successivamente lo si ricrea, i resolver DNS memorizzeranno nella cache la risposta negativa (questo record non esiste) per un periodo più lungo. In questo modo si allungano i tempi in cui i clienti o gli utenti non possono raggiungere la risorsa corrispondente, ad esempio un server Web per acme.example.com.

Per trovare i record SOA in Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Seleziona il nome collegato del dominio per cui desideri visualizzare i record.
4. Nella sezione Records (Record) puoi visualizzare tutti i record elencati e puoi filtrarli in modo da trovare il valore del tuo SOA.

Utilizzo delle zone ospitate private

Una zona ospitata privata è un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPCs domini creati con il servizio Amazon VPC. Di seguito viene descritto il funzionamento delle zone ospitate private:

1. Puoi creare una zona ospitata privata, come esempio.com, e specificare il VPC che desideri associare alla zona ospitata. Dopo aver creato la zona ospitata, puoi associarne altre. VPCs
2. Crei record nella zona ospitata che determinano in che modo Route 53 risponde alle query DNS per il tuo dominio e i sottodomini all'interno e tra i tuoi. VPCs Ad esempio, supponiamo di avere un server di database eseguito su un' EC2 istanza nel VPC che hai associato alla tua zona ospitata privata. Puoi creare un record A o AAAA, ad esempio db.esempio.com e specificare l'indirizzo IP del server di database.

   Per ulteriori informazioni sul record, consulta Utilizzo dei record. Per informazioni sui requisiti di Amazon VPC per l'utilizzo di zone ospitate private, consulta Utilizzo di zone ospitate private nella Guida per l'utente di Amazon VPC.
3. Quando un'applicazione inoltra una query DNS per db.esempio.com, Route 53 restituisce l'indirizzo IP corrispondente. Per ottenere una risposta da una zona ospitata privata, è inoltre necessario eseguire un'EC2 istanza in una delle aree associate VPCs (o disporre di un endpoint in entrata da una configurazione ibrida). Se provi a interrogare una zona ospitata privata dall'esterno della configurazione VPCs o della configurazione ibrida, la query verrà risolta in modo ricorsivo su Internet.
4. L'applicazione utilizza l'indirizzo IP che ha ricevuto da Route 53 per stabilire una connessione con il server di database.

Quando crei una zona ospitata privata, vengono utilizzati i seguenti server nomi:

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

Questi server nomi vengono utilizzati perché il protocollo DNS richiede che ogni zona ospitata disponga di un set di record NS. Questi server nomi sono riservati e non vengono mai utilizzati dalle zone ospitate pubbliche di Route 53. È possibile interrogare tali zone solo tramite Route 53 Resolver in un VPC che è stato associato alla zona ospitata utilizzando un endpoint in ingresso connesso a quello VPCs specificato nella zona ospitata privata.

Sebbene i server dei nomi siano visibili su Internet, Route 53 Resolver non si connette agli indirizzi di tale server. Inoltre, le informazioni sulle zone ospitate private non vengono restituite se si esegue una query direttamente sui server dei nomi tramite Internet. Al contrario, Route 53 Resolver rileva la presenza di quey all'interno di uno spazio dei nomi privato basato su associazioni di zone ospitate e VPC e utilizza la connettività privata diretta per raggiungere i server DNS privati.

> **Note**
>
> Se lo desideri, puoi modificare il set di record NS in una zona ospitata privata senza compromettere il funzionamento della risoluzione DNS privata. Se decidi di eseguire questa operazione, sebbene non sia consigliata, scegli nomi di dominio riservati che non vengono utilizzati dai server DNS pubblici.

Se desideri instradare il traffico per il tuo dominio su Internet, utilizza una zona ospitata pubblica di Route 53. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate pubbliche.

Argomenti

- Dissociarsi VPCs da una zona ospitata privata
- Eliminazione di una zona ospitata privata
- Autorizzazioni VPC

Considerazioni sull'utilizzo di una zona ospitata privata

Quando usi le zone ospitate private, tieni in considerazione quanto segue:

- 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

Impostazioni di Amazon VPC

Per usare zone ospitate private, devi impostare le seguenti impostazioni di Amazon VPC su `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Per ulteriori informazioni, consulta Visualizza e aggiorna gli attributi DNS per il tuo VPC nella Amazon VPC User Guide.

Controllo dell'integrità di Route 53

In una zona ospitata privata, puoi associare i controlli di integrità di Route 53 solo ai record di failover, risposta multivalore, ponderata, latenza, geolocalizzazione e geoprossimità. Per ulteriori informazioni sull'associazione di controlli dell'integrità con record di failover, consulta Configurazione del failover in una zona ospitata privata.

Policy di routing supportate per i record in una zona ospitata privata

Puoi utilizzare le seguenti policy di routing al momento della creazione di un record in una zona ospitata privata:

- Routing semplice
- Routing di failover
- Routing di risposta multivalore
- Routing ponderato
- Routing basato sulla latenza
- Routing di geolocalizzazione
- Routing di geoprossimità

La creazione di record in una zona ospitata privata utilizzando altre policy di routing non è supportata.

Visualizzazione doppia di DNS

Puoi utilizzare Route 53 per configurare DNS con visualizzazione separata, noto anche come DNS split-horizon. Nella visualizzazione doppia di DNS, utilizzi lo stesso nome di dominio (esempio.com) per usi interni (accounting.esempio.com) ed esterni, ad esempio il tuo sito Web pubblico (www.esempio.com). Potrebbe anche essere necessario utilizzare lo stesso nome di sottodominio internamente ed esternamente, ma servire contenuti diversi o richiedere un'autenticazione diversa per gli utenti interni ed esterni.

Per configurare la visualizzazione doppia di DNS, esegui la procedura seguente:

1. Crea zone ospitate pubbliche e private con lo stesso nome. (La visualizzazione doppia di DNS funziona ancora se utilizzi un altro servizio DNS per la zona ospitata pubblica.)
2. Associa uno o più Amazon VPCs alla zona ospitata privata. Route 53 Resolver utilizza la zona ospitata privata per instradare le query DNS nella zona specificata. VPCs
3. Crea record in ogni zona ospitata. I record nella zona ospitata pubblica controllano il modo in cui viene instradato il traffico Internet e i record nella zona ospitata privata controllano il modo in cui viene instradato il traffico su Amazon. VPCs

Se è necessario eseguire la risoluzione dei nomi dei carichi di lavoro VPC e on-premise, puoi utilizzare Route 53 Resolver. Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.

Zone ospitate pubbliche e private con spazi dei nomi sovrapposti

Se si dispone di zone ospitate pubbliche e private con spazi dei nomi sovrapposti, ad esempio example.com e accounting.example.com, Resolver instrada il traffico in base alla corrispondenza più specifica. Quando gli utenti accedono a un' EC2 istanza in un Amazon VPC che hai associato alla zona ospitata privata, ecco come Route 53 Resolver gestisce le query DNS:

1. Resolver valuta se il nome della zona ospitata privata corrisponde al nome di dominio nella richiesta, ad esempio accounting.esempio.com. Una corrispondenza è definita come segue:
   - Una corrispondenza identica
   - Il nome della zona ospitata privata è un elemento padre del nome di dominio nella richiesta. Ad esempio, supponiamo che il nome di dominio della richiesta sia il seguente:

     seattle.accounting.esempio.com

     Le seguenti zone ospitate corrispondono perché sono elementi padre di seattle.accounting.esempio.com:
     - accounting.esempio.com
     - esempio.com

   Se non esiste alcuna zona ospitata privata corrispondente, allora il Resolver inoltra la richiesta a un resolver DNS pubblico e la richiesta viene risolta come una normale query DNS.
2. Se esiste un nome di zona ospitata privata che corrisponde al nome di dominio nella richiesta, nella zona ospitata viene ricercato un record che corrisponde al nome di dominio DNS e al tipo della richiesta, ad esempio un record per accounting.esempio.com.

   > **Note**
   >
   > Se è presente una zona ospitata privata corrispondente ma non esiste un record corrispondente al nome e al tipo di dominio della richiesta, Resolver non inoltra la richiesta a un resolver DNS pubblico. Al contrario, restituisce NXDOMAIN (dominio inesistente) al client.

Zone ospitate pubbliche e private con spazi dei nomi sovrapposti

Se si dispone di due o più zone ospitate private con spazi dei nomi sovrapposti, ad esempio esempio.com e accounting.esempio.com, Resolver instrada il traffico in base alla corrispondenza più specifica.

> **Note**
>
> Se si dispone di una zona privata ospitata (esempio.com) e di una regola di Route 53 Resolver che instrada il traffico alla rete per lo stesso nome di dominio, la regola del Resolver ha la precedenza. Per informazioni, consulta Private hosted zones and Route 53 Resolver rules.

Quando gli utenti accedono a un' EC2 istanza in un Amazon VPC che hai associato a tutte le zone ospitate private, ecco come Resolver gestisce le query DNS:

1. Resolver valuta se il nome dominio nella richiesta, ad esempio accounting.esempio.com, corrisponde al nome di una delle zone ospitate private.
2. In assenza di una zona ospitata che corrisponde esattamente al nome di dominio nella richiesta, Resolver verifica la presenza di una zona ospitata con un nome che è un elemento padre del nome di dominio nella richiesta. Ad esempio, supponiamo che il nome di dominio della richiesta sia il seguente:

   `seattle.accounting.example.com`

   Le seguenti zone ospitate corrispondono perché sono elementi padre di `seattle.accounting.example.com`:

   - `accounting.example.com`
   - `example.com`

   Resolver sceglie `accounting.example.com` perché è più specifico di `example.com`.
3. Resolver ricerca nella zona ospitata `accounting.example.com` un record che corrisponda al nome di dominio e al tipo DNS nella richiesta, ad esempio un record A per `seattle.accounting.example.com`.

   Se non è presente un record che corrisponde al nome e al tipo di dominio nella richiesta, Resolver restituisce NXDOMAIN (dominio inesistente) al client.

Regole di zone ospitate private e Route 53 Resolver

Se disponi di una zona ospitata privata (esempio.com) e di una regola di Route 53 Resolver che instrada il traffico alla rete per lo stesso nome di dominio, la regola del Resolver ha la precedenza.

Si prenda come esempio la seguente configurazione:

- Hai una zona ospitata privata denominata example.com che associ a un VPC.
- Crea una regola Route 53 Resolver che inoltri il traffico di esempio.com alla rete e associ la regola allo stesso VPC.

In questa configurazione, la regola del Resolver ha la priorità rispetto alla zona ospitata privata. Le query DNS vengono inoltrate alla rete anziché risolte in base ai record nella zona ospitata privata.

Delegare responsabilità per un sottodominio

Non puoi creare record NS in una zona ospitata privata per delegare responsabilità per un sottodominio.

Server DNS personalizzati

Se hai configurato server DNS personalizzati su EC2 istanze Amazon nel tuo VPC, devi configurare tali server DNS per instradare le tue query DNS private all'indirizzo IP dei server DNS forniti da Amazon per il tuo VPC. Questo indirizzo IP è l'indirizzo IP alla base dell'intervallo di rete VPC "più due". Ad esempio, se l'intervallo di CIDR per il tuo VPC è 10.0.0.0/16, l'indirizzo IP del server DNS è 10.0.0.2.

Se desideri instradare le query DNS tra e la tua rete, puoi utilizzare Resolver. VPCs Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.

Autorizzazioni IAM richieste

Per creare zone private ospitate, devi concedere le autorizzazioni IAM per EC2 le azioni Amazon oltre alle autorizzazioni per le azioni Route 53. Per ulteriori informazioni, consulta Operazioni, risorse e chiavi di condizione per Route 53 in Service Authorization Reference.

Creazione di una zona ospitata privata

Una zona ospitata privata è un contenitore per i record di un dominio ospitato in uno o più cloud privati virtuali Amazon (VPCs). Crei una zona ospitata per un dominio (ad esempio example.com), quindi crei record per indicare ad Amazon Route 53 come desideri che il traffico venga instradato per quel dominio all'interno e tra i tuoi. VPCs

> **Important**
>
> Quando crei una zona ospitata privata, devi associare un VPC alla zona ospitata e il VPC specificato deve essere stato creato utilizzando lo stesso account che utilizzi per creare la

zona ospitata. Dopo aver creato la zona ospitata, puoi associarne altri VPCs , inclusa VPCs quella creata utilizzando un account diverso. AWS
Per associare VPCs quella creata utilizzando un account a una zona ospitata privata creata utilizzando un account diverso, è necessario autorizzare l'associazione e quindi creare l'associazione a livello di codice. Per ulteriori informazioni, consulta Associazione di un Amazon VPC e una zona ospitata privata creata con account diversi AWS.

Per informazioni su come creare una zona ospitata privata tramite l'API Route 53, consulta la Documentazione di riferimento delle API di Amazon Route 53.

Come creare una zona ospitata privata tramite la console Route 53

1. Per ogni VPC che desideri associare alla zona ospitata di Route 53, modifica le seguenti impostazioni di VPC in `true`:

   - `enableDnsHostnames`
   - `enableDnsSupport`

   Per ulteriori informazioni, consultare Aggiornamento del supporto DNS per il VPC nella Guida per l'utente di Amazon VPC.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
3. I nuovi utenti di Route 53 possono consultare Nozioni di base.

   Se stai già utilizzando Route 53, scegli Zone ospitate nel pannello di navigazione.
4. Scegli Crea zona ospitata.
5. Nel riquadro Crea zona ospitata privata, inserisci un nome di dominio e, facoltativamente, un commento.

   Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.
6. Nell'elenco Tipo, scegli Zona ospitata privata.
7. Nell'elenco VPC ID (ID VPC), scegli il VPC che desideri associare alla zona ospitata.

> **Note**
>
> Se la console mostra il seguente messaggio, stai tentando di associare una zona ospitata che utilizza lo stesso spazio dei nomi di quello di un'altra zona ospitata all'interno dello stesso VPC:
> "Un dominio in conflitto è già associato a un determinato VPC o set di delega".
> Ad esempio, se la zona ospitata A e la zona ospitata B utilizzano entrambi lo stesso nome di dominio, come `example.com`, non è possibile associare entrambe le zone ospitate allo stesso VPC.

8. Scegli Crea zona ospitata.

Elencare zone ospitate private

Puoi utilizzare la console Amazon Route 53 per elencare tutte le zone ospitate che hai creato con l' AWS account corrente. Per informazioni su come elencare le zone ospitate utilizzando l'API Route 53, ListHostedZonesconsulta Amazon Route 53 API Reference.

Per elencare le zone ospitate associate a un AWS account

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.

   La pagina Hosted Zones mostra automaticamente un elenco di tutte le zone ospitate che sono state create utilizzando l' AWS account corrente. La colonna Type (Tipo) indica se una zona ospitata è privata o pubblica. Scegli l'intestazione di colonna per raggruppare tutte le zone ospitate private e pubbliche.

Associarne di più VPCs a una zona ospitata privata

Puoi utilizzare la console Amazon Route 53 per VPCs associare altre informazioni a una zona ospitata privata se hai creato la zona ospitata e VPCs poi utilizzando lo stesso AWS account.

> **Important**
>
> Se desideri associare VPCs ciò che hai creato utilizzando un account a una zona ospitata privata creata utilizzando un account diverso, devi prima autorizzare l'associazione. Inoltre, non è possibile utilizzare la AWS console per autorizzare l'associazione o associarla alla zona VPCs ospitata. Per ulteriori informazioni, consulta Associazione di un Amazon VPC e una zona ospitata privata creata con account diversi AWS.

Per informazioni su come associare di più VPCs a una zona ospitata privata utilizzando l'API Route 53, consulta Associate VPCWith HostedZone nel riferimento all'API di Amazon Route 53.

Per associarne altre VPCs a una zona ospitata privata utilizzando la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il pulsante di opzione per la zona ospitata privata a cui desideri associarti di più VPCs .
4. Scegli Modifica.
5. Scegli Aggiungi VPC.
6. Scegli la regione e l'ID del VPC che desideri associare alla zona ospitata.
7. Per VPCs associare altre informazioni a questa zona ospitata, ripeti i passaggi 5 e 6.
8. Scegli Save changes (Salva modifiche).

Associazione di un Amazon VPC e una zona ospitata privata creata con account diversi AWS

Se desideri associare un VPC creato con un AWS account a una zona ospitata privata creata con un account diverso, esegui la seguente procedura:

Per associare un Amazon VPC e una zona ospitata privata creata con account diversi AWS

1. Utilizzando l'account che ha creato la zona ospitata, autorizza l'associazione del VPC con la zona ospitata privata utilizzando uno dei seguenti metodi:
   - AWS CLI— Vedi create-vpc-association-authorizationnel riferimento ai AWS CLI comandi

- AWS SDK o AWS Tools for Windows PowerShell: consulta la documentazione applicabile nella pagina AWS Documentazione
- API Amazon Route 53: consulta Create VPCAssociation Authorization nel riferimento all'API Amazon Route 53

Tieni presente quanto segue:

- Se desideri associare più VPCs account creati con un account a una zona ospitata creata con un account diverso, devi inviare una richiesta di autorizzazione per ogni VPC.
- Quando autorizzi l'associazione, devi specificare l'ID della zona ospitata, perciò la zona ospitata privata deve esistere già.
- Non puoi utilizzare la console Route 53 per autorizzare l'associazione di un VPC con una zona ospitata privata o per effettuare l'associazione.

2. Utilizzando l'account che ha creato il VPC, associa il VPC alla zona ospitata. Oltre all'autorizzazione dell'associazione, puoi utilizzare l' AWS SDK, Tools for Windows PowerShell o l'API AWS CLI Route 53. Se utilizzi l'API, utilizza l'azione Associa VPCWith HostedZone.
3. Consigliato: elimina l'autorizzazione per associare il VPC alla zona ospitata. L'eliminazione di un'autorizzazione non interessa l'associazione, ma semplicemente impedisce la nuova associazione del VPC con la zona ospitata in futuro. Se desideri riassociare il VPC alla zona ospitata, devi ripetere i passaggi 1 e 2 di questa procedura.

> **Important**
>
> `ListHostedZonesByVPC`restituisce le zone ospitate fornite da un VPC e l'`GetHostedZone`API restituisce la zona VPCs associata alla zona ospitata. Questi considerano APIs solo l'associazione tra zona ospitata e VPC creata dall'`AssociateVPCWithHostedZone`API o quando viene creata la zona ospitata privata. Se desideri un elenco completo delle associazioni di zone ospitate su un VPC, chiama anche. ListProfileResourceAssociations

> **Note**
>
> Per il numero massimo di autorizzazioni che puoi creare, consulta Quote relative alle entità.

Dissociarsi VPCs da una zona ospitata privata

Puoi utilizzare la console Amazon Route 53 per dissociarti VPCs da una zona ospitata privata. In questo modo Route 53 causa l'arresto del traffico di routing utilizzando i record nella zona ospitata per le query DNS originate nel VPC. Ad esempio, se la zona ospitata esempio.com è associata a un VPC e la si dissocia da tale VPC, Route 53 interrompe la risoluzione delle query DNS per esempio.com o uno qualsiasi degli altri record nella zona ospitata esempio.com.

> **Note**
>
> Non è possibile disassociare l'ultimo VPC da una zona privata ospitata. Se si desidera dissociare tale VPC, è innanzitutto necessario associare un altro VPC alla zona ospitata.

Per dissociarsi VPCs da una zona ospitata privata

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il pulsante di opzione per la zona ospitata privata da cui desideri dissociarti VPCs da una o più zone.
4. Scegli Modifica.
5. Scegli Rimuovi VPC accanto al VPC che desideri dissociare da questa zona ospitata.
6. Scegli Save changes (Salva modifiche).

Eliminazione di una zona ospitata privata

In questa sezione viene spiegato come eliminare una zona ospitata privata utilizzando la console Amazon Route 53.

Puoi eliminare una zona ospitata privata solo se non sono presenti record diversi dai record SOA e NS di default. Se la tua zona ospitata contiene altri record, devi eliminarli prima di eliminare la zona ospitata. In questo modo si impedisce l'eliminazione accidentale di una zona ospitata che contiene ancora record.

Argomenti

Eliminazione di zone ospitate private create da un altro servizio

Se una zona ospitata privata è stata creata da un altro servizio, non sarà possibile eliminarla mediante la console Route 53. Al contrario, è necessario utilizzare il processo applicabile all'altro servizio:

- AWS Cloud Map— Per eliminare una zona ospitata AWS Cloud Map creata quando hai creato uno spazio dei nomi DNS privato, elimina lo spazio dei nomi. AWS Cloud Map elimina automaticamente la zona ospitata. Per ulteriori informazioni, consulta Eliminazione degli spazi dei nomi nella Guida per gli sviluppatori di AWS Cloud Map .
- Rilevamento del servizio Amazon Elastic Container Service (Amazon ECS): per eliminare una zona ospitata privata creata da Amazon ECS quando hai creato un servizio utilizzando l'individuazione dei servizi, eliminare i servizi Amazon ECS che utilizzano lo spazio dei nomi ed eliminare lo spazio dei nomi. Per ulteriori informazioni, consulta Eliminazione di un servizio nella Guida per gli sviluppatori di Amazon Elastic Container Service.

Utilizzo della console di Route 53 per eliminare una zona ospitata privata

Per utilizzare la console Route 53 per eliminare una zona ospitata privata, completa la procedura seguente.

Utilizzo della console di Route 53 per eliminare una zona ospitata privata

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Conferma che la zona ospitata che desideri eliminare contiene solo un record NS e un record SOA. Se contiene record aggiuntivi, eliminali:

   a. Seleziona il nome della zona ospitata che desideri eliminare.

   b. Nella pagina Record, se l'elenco dei record include i record per i quali il valore della colonna Tipo è diverso da NS o SOA, scegli la riga, quindi seleziona Elimina.

      Per selezionare più record consecutivi, seleziona la prima riga, tieni premuto il tasto Shift (MAIUSC) e seleziona l'ultima riga. Per selezionare più record non consecutivi, seleziona la prima riga, tieni premuto il tasto Ctrl e seleziona le righe rimanenti.

3. Nella pagina Hosted zone, scegli la riga per la zona ospitata che desideri eliminare.
4. Scegli Elimina.
5. Digita la chiave di conferma e scegli Elimina.

Autorizzazioni VPC

Le autorizzazioni VPC utilizzano la condizione dei criteri di gestione delle identità e degli accessi (IAM) per consentire di impostare autorizzazioni granulari per VPCs quando si utilizza Associate VPCWithHostedZone, Disassociate VPCFrom HostedZone, Create Authorization, Delete VPCAssociation Authorization e VPC. VPCAssociation CreateHostedZoneListHostedZonesBy APIs

Con la condizione della policy IAM`route53:VPCs`, puoi concedere diritti amministrativi granulari ad altri utenti. AWS Ciò consente di concedere a qualcuno le autorizzazioni per associare una zona ospitata, dissociare dalla zona ospitata, creare l'autorizzazione di associazione VPC per, eliminare l'autorizzazione all'associazione VPC per, creare una zona ospitata o elencare le zone ospitate per:

- Un singolo VPC.
- Qualsiasi VPCs all'interno della stessa regione.
- Multiplo VPCs.

Per ulteriori informazioni sulle autorizzazioni VPC, consulta. Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi

Per informazioni su come autenticare AWS gli utenti, vedi Autenticazione con identità e per sapere come controllare l'accesso alle risorse di Route 53, vedi. Controllo accessi

Migrazione di una zona ospitata su un altro account AWS

Se desideri migrare una zona ospitata da un AWS account a un altro account, puoi elencare a livello di codice i record nella vecchia zona ospitata, modificare l'output e quindi creare a livello di codice i record in una nuova zona ospitata utilizzando l'output modificato. Tieni presente quanto segue:

- Se disponi solo di pochi record, puoi usare la console Route 53 anche per creare i record nella nuova zona ospitata. Per ulteriori informazioni, consulta Creazione di record utilizzando la console Amazon Route 53.
- Alcune procedure utilizzano il (). AWS Command Line Interface AWS CLI Puoi anche eseguire queste procedure utilizzando una delle AWS SDKs, l'API Amazon Route 53 o AWS Tools for

Windows PowerShell. Per questo argomento, utilizziamo il AWS CLI perché è più facile per un numero limitato di zone ospitate.

- Puoi inoltre utilizzare questa procedura per creare record in una nuova zona ospitata con un nome diverso rispetto a una zona ospitata esistente ma con gli stessi record.
- Non puoi migrare record alias che instradano il traffico verso le istanze di policy di traffico.

Argomenti

Passaggio 1: installa o aggiorna AWS CLI

Per informazioni sul download, l'installazione e la configurazione di AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

> **Note**
>
> Configura la CLI in modo che sia possibile utilizzarla quando stai utilizzando sia l'account che ha creato la zona ospitata sia l'account su cui stai migrando la zona ospitata. Per ulteriori informazioni, consulta Configurazione nella Guida per l'utente di AWS Command Line Interface .

Se stai già utilizzando AWS CLI, ti consigliamo di eseguire l'aggiornamento alla versione più recente della CLI in modo che i comandi CLI supportino le funzionalità più recenti di Route 53.

Fase 2: crea una nuova zona ospitata

La procedura seguente spiega come utilizzare la console Route 53 per creare la zona ospitata a c ui si desidera migrare.

> **Note**
>
> Route 53 assegna un nuovo set di quattro server dei nomi alla nuova zona ospitata. Dopo aver migrato una zona ospitata su un altro AWS account, è necessario aggiornare la registrazione del dominio per utilizzare i name server per la nuova zona ospitata. Ti ricorderemo questo passaggio più tardi.

Per creare la nuova zona ospitata utilizzando un account diverso

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Accedi con le credenziali dell'account per l'account su cui desideri migrare la zona ospitata.
2. Crea una zona ospitata. Per ulteriori informazioni, consulta Creazione di una zona ospitata pubblica.
3. Annota l'ID della zona ospitata. In alcuni casi, avrai bisogno di queste informazioni in un secondo momento.
4. Esci dalla console Route 53.

Fase 3: crea un file che contiene i record da migrare

Per eseguire la migrazione dei record da una zona ospitata a un'altra, è necessario creare un file che contiene i record che desideri migrare, modificare il file e quindi utilizzare il file modificato per creare record nella nuova zona ospitata. Per creare il file, esegui la procedura descritta di seguito.

Per creare un file che contiene i record da migrare

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/

   Accedere con le credenziali dell'account per l'account che ha creato la zona ospitata che si desidera migrare.

2. Individuare l'ID della zona ospitata per la zona ospitata che si desidera migrare:

   a. Nel pannello di navigazione, scegli Zone ospitate.

   b. Trovare la zona ospitata che si desidera migrare. Se hai molte zone ospitate, puoi scegliere Nome dominio esatto e immettere il nome della zona ospitata, quindi premere Invio per filtrare l'elenco.

   c. Individuare il valore della colonna zona ospitata ID (ID zona ospitata).

3. Esegui il comando seguente:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

   Tieni presente quanto segue:

   - Per*hosted-zone-id*, specifica l'ID della zona ospitata che hai ottenuto nel passaggio 2 di questa procedura.
   - Per*path-to-output-file*, specifica il percorso della directory e il nome del file in cui vuoi salvare l'output.
   - Il carattere > invia l'output al file specificato.
   - Gestisce AWS CLI automaticamente l'impaginazione per le zone ospitate che contengono più di 100 record. Per ulteriori informazioni, vedere Utilizzo delle opzioni di impaginazione dell'interfaccia a riga di AWS comando nella Guida per l'AWS Command Line Interface utente.

     Se si utilizza un altro metodo programmatico per elencare i record, ad esempio uno dei seguenti AWS SDKs, è possibile ottenere un massimo di 100 record per pagina di risultati. Se la zona ospitata contiene più di 100 record, è necessario inviare più richieste per elencare tutti i record.
   - Per eseguire il comando nelle versioni di Windows PowerShell precedenti alla 6.0, utilizzare la sintassi seguente:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
```

   Ad esempio, se si esegue AWS CLI su un computer Windows, è possibile eseguire il comando seguente:

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp
\list-records-ZOLDZONE12345.txt
```

Se lo esegui AWS CLI su un computer Windows in una versione di Windows PowerShell precedente alla 6.0, puoi eseguire il comando seguente:

```
$output = aws route53 list-resource-record-sets --hosted-zone-id <hosted-zone-id>;
 $mypath = <output-path ;
[System.IO.File]::WriteAllLines($mypath,$output)
```

4. Creare una copia di questo output. Dopo aver creato i record nella nuova zona ospitata, è consigliabile eseguire il AWS CLI `list-resource-record-sets` comando sulla nuova zona ospitata e confrontare i due output per assicurarsi che tutti i record siano stati creati.

Fase 4: modifica i record da migrare

Il formato del file creato nella procedura precedente è simile al formato richiesto dal AWS CLI `change-resource-record-sets` comando utilizzato per creare record nella nuova zona ospitata. Tuttavia, il file richiede alcune modifiche. È necessario applicare alcune delle modifiche a ogni record. È possibile effettuare queste modifiche utilizzando la funzione di ricerca e sostituzione in un buon editor di testo.

Aprire una copia del file creato in Fase 3: crea un file che contiene i record da migrare e apportare le modifiche seguenti:

- Eliminare le prime due righe nella parte superiore dell'output:

```
{
    "ResourceRecordSets": [
```

- Eliminare le righe correlate ai record NS e SOA. La nuova zona ospitata dispone già di tali record.
- Opzionale: aggiungi un elemento `Comment`.
- Aggiungere un elemento `Changes`.
- Per ogni record, aggiungere un elemento `Action` e `ResourceRecordSet`.
- Aggiungere parentesi graffe di apertura e chiusura (`{ }`) come richiesto per rendere il codice JSON valido.

> **Note**
>
> È possibile usare un validatore JSON per verificare che tutte le graffe e le parentesi siano nella posizione corretta. Per trovare un validatore JSON online, eseguire una ricerca su Internet utilizzando la query "`json validator`".

- Se la zona ospitata contiene eventuali alias che fanno riferimento ad altri record nella stessa zona ospitata, apportare le modifiche seguenti:
  - Cambiare l'ID della zona ospitata con l'ID della nuova zona ospitata.

    > **Important**
    >
    > Se il record di alias punta a un'altra risorsa, ad esempio un sistema di bilanciamento del carico, non modificate l'ID della zona ospitata con l'ID della zona ospitata del dominio. Se modifichi accidentalmente l'ID della zona ospitata, ripristina l'ID della zona ospitata sull'ID della zona ospitata della risorsa stessa, non sull'ID della zona ospitata del dominio. L'ID della zona ospitata può essere trovato dalla console AWS in cui è stata creata la risorsa.

  - Sposta i record alias alla fine del file. Prima di poter creare il record alias, Route 53 deve creare il record a cui un record alias fa riferimento.

    > **Important**
    >
    > Se uno o più record alias fanno riferimento ad altri record alias, i record che rappresentano la destinazione di alias devono comparire nel file prima dei record alias di riferimento. Ad esempio, se `alias.example.com` è l'alias di destinazione per `alias.alias.example.com`, `alias.example.com` deve apparire primo nel file.

  - Eliminare i record alias che instradano il traffico verso un'istanza di policy di traffico. Annotare i record in modo da ricrearli più tardi.
- È possibile utilizzare questa procedura per creare record in una zona ospitata con un nome diverso. Per ogni record nell'output, modificare la parte del nome di dominio dell'elemento `Name` con il nome della nuova zona ospitata. Ad esempio, se si elencano record nella zona ospitata esempio.com e si desidera creare record in una zona ospitata esempio.net, modificare la parte esempio.com di ogni nome record in esempio.net:

  Da:

- "Name": "example.com."
- "Name": "www.example.com."

A:

- "Name": "example.net."
- "Name": "www.example.net."

L'esempio seguente mostra la versione modificata dei record per una zona ospitata per esempio.com. Il testo rosso in corsivo è nuovo:

```
{
    "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."
            }
        }
    ]
}
```

Fase 5: dividi i file di grandi dimensioni in file più piccoli

Se si dispone di una notevole quantità di record o se si dispone di record che hanno molti valori (ad esempio, molti indirizzi IP), potrebbe essere necessario suddividere il file in file più piccoli. Di seguito i valori massimi:

- Ogni file può contenere un massimo di 1.000 record.
- La lunghezza combinata massima dei valori di tutti gli elementi `Value` è 32.000 byte.

Fase 6: crea record nella nuova zona ospitata

Per creare record nella nuova zona ospitata, utilizzate il seguente AWS CLI comando:

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-new-hosted-zone --
change-batch file://path-to-file-that-contains-records
```

Per esempio:

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch
 file://c:/temp/change-records-ZNEWZONE1245.txt
```

Se hai eliminato alcun record alias che instradano il traffico verso un'istanza di policy di traffico, crearli nuovamente utilizzando la console Route 53. Per ulteriori informazioni, consulta Creazione di record utilizzando la console Amazon Route 53.

Fase 7: confronta i record nelle vecchie e nelle nuove zone ospitate

Per confermare di aver creato correttamente tutti i record nella nuova zona ospitata, consigliamo di elencare i record nella nuova zona ospitata e di confrontare l'output con l'elenco dei record della vecchia zone ospitata. A questo scopo, esegui la procedura seguente.

Per confrontare i record nelle vecchie e nuove zone ospitate

1. Esegui il comando seguente:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json
 > path-to-output-file
```

Specifica i seguenti valori:

- Per*hosted-zone-id*, specifica l'ID della nuova zona ospitata.
- Per*path-to-output-file*, specifica il percorso della directory e il nome del file in cui vuoi salvare l'output. Usare un nome del file diverso dal nome del file utilizzato in Fase 3: crea un file che contiene i record da migrare. L'utilizzo di un nome del file diverso garantisce che il nuovo file non sovrascriverà il file precedente.
- Il carattere > invia l'output al file specificato.

Ad esempio, se si sta utilizzando un computer Windows, è possibile eseguire il comando seguente:

```
aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json
 > c:\temp\list-records-ZNEWZONE67890.txt
```

2. Confrontare l'output con l'output proveniente da Fase 3: crea un file che contiene i record da migrare.

   Oltre ai valori dei record NS e SOA e alle eventuali modifiche apportate Fase 4: modifica i record da migrare (ad esempio zone ospitate IDs o nomi di dominio diversi), i due output devono essere identici.

3. Se i record nella nuova zona ospitata non corrispondono ai record nella vecchia zona ospitata, è possibile procedere in uno dei seguenti modi:

   - Effettuare correzioni minori utilizzando la console Route 53. Per ulteriori informazioni, consulta Modifica di record.
   - Se un numero elevato di record risultano mancanti, creare un nuovo file di testo che contiene i record mancanti e quindi ripetere Fase 6: crea record nella nuova zona ospitata.
   - Eliminare tutti i record ad eccezione dei record NS e SOA nella nuova zona ospitata e ripetere i seguenti passaggi:
     - Fase 4: modifica i record da migrare
     - Fase 5: dividi i file di grandi dimensioni in file più piccoli

- Fase 6: crea record nella nuova zona ospitata
- Fase 7: confronta i record nelle vecchie e nelle nuove zone ospitate

Fase 8: aggiorna la registrazione del dominio in modo che utilizzi i server di nomi per la nuova zona ospitata

Quando è terminata la creazione di record nella nuova zona ospitata, modificare i server di nomi per la registrazione del dominio in modo che utilizzi i server di nomi per la nuova zona ospitata.

> **Important**
>
> Se non aggiorni la registrazione del dominio in modo che utilizzi i server di nomi per la nuova zona ospitata, per instradare il traffico del dominio Route 53 continuerà a utilizzare le vecchie zone ospitate. Se si cancella la vecchia zona ospitata senza aggiornare i server di nomi per la registrazione del dominio, il dominio non sarà disponibile su Internet. Se si aggiungono, aggiornano o eliminano i record nella nuova zona ospitata senza aggiornare i server di nomi per la registrazione del dominio, il traffico non sarà instradato in base a tali modifiche.

Per ulteriori informazioni, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

> **Note**
>
> Se si utilizza il processo per migrare il servizio DNS per un dominio utilizzato o il processo per un dominio inattivo, è possibile saltare i seguenti passaggi perché sono già stati creati una nuova zona ospitata e i relativi record:
>
> - Fase 1: ottieni la tua attuale configurazione DNS dal fornitore di servizi DNS attuale
> - Fase 2: crea una hosted zone
> - Fase 3: crea record

Fase 9: attendi che i resolver DNS inizino a utilizzare la nuova zona ospitata

Se il dominio è in uso, per esempio se gli utenti utilizzano il nome di dominio per navigare in un sito Web o accedere a un'applicazione Web, allora i resolver DNS hanno memorizzati nella cache i nomi

del server di nomi che è stato fornito dal tuo attuale provider di servizi DNS. Un resolver DNS che ha memorizzato nella cache tali informazioni da pochi minuti le salverà per al massimo due giorni.

> **Note**
>
> Se è stato creato un record nella nuova zona ospitata che non è presente nella vecchia zona ospitata, gli utenti non sono in grado di utilizzare il nuovo record per accedere alle risorse finché i resolver non iniziano a usare i server di nomi per la nuova zona ospitata. Ad esempio, supponiamo di creare un record, test.esempio.com, nella nuova zona ospitata che deve instradare il traffico Internet sul proprio sito Web. Se il record non viene visualizzato nella vecchia zona ospitata, non potrai immettere test.esempio.com in un browser Web finché i resolver non iniziano a usare la nuova zona ospitata.

Per assicurarti che la migrazione di una zona ospitata su un altro AWS account sia completata prima di eliminare la vecchia zona ospitata, attendi due giorni dopo l'aggiornamento della registrazione del dominio per utilizzare i name server per la nuova zona ospitata.

> **Note**
>
> Il valore TTL predefinito è 172800 secondi (2 giorni). È possibile modificare questo valore in modo che sia più breve. Per ulteriori informazioni, consulta TTL (secondi).

Dopo che il TTL di due giorni scade e i resolver richiedono i server di nomi per il tuo dominio, i resolver otterranno i server di nomi attuali. Puoi inoltre abilitare Registrazione delle query di Resolver per monitorare le query nelle nuove zone ospitate. Per ulteriori informazioni sulle tariffe della registrazione delle query del risolutore, consulta la pagina Tariffe di CloudWatch .

Fase 10: (opzionale) elimina la vecchia zona ospitata

Quando si è certi che la vecchia zona ospitata non è più necessaria più, è possibile facoltativamente eliminarla.

> **Important**
>
> Non eliminare la vecchia zona ospitata o qualsiasi record in quella zona ospitata per almeno 48 ore dopo l'aggiornamento della registrazione del dominio in modo che utilizzi i server di

nomi per la nuova zona ospitata. Se si cancella la vecchia zona ospitata prima che i resolver DNS interrompano l'utilizzo dei record in quella zona ospitata, il dominio potrebbe essere non disponibile su Internet finché i resolver non iniziano a usare la nuova zona ospitata.

La zona ospitata deve essere vuota ad eccezione dei record NS e SOA. Se la vecchia zona ospitata contiene numerosi record, eliminarli utilizzando la console può richiedere molto tempo. Un'opzione è procedere nel seguente modo:

1. Creare un'altra copia del file modificato da Fase 4: modifica i record da migrare.
2. Nella copia del file, modificare `"Action": "CREATE"` a `"Action": "DELETE"` per ogni record.
3. Utilizzate il seguente AWS CLI comando per eliminare i record:

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --
change-batch file:///path-to-file-that-contains-records
```

> **Important**
>
> Assicurarsi che il valore specificato per l'ID zona ospitata sia l'ID della vecchia zona ospitata, non l'ID della nuova zona ospitata.

4. Eliminare i record rimanenti e la zona ospitata:

   a. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

      Accedere con le credenziali dell'account per l'account che ha creato la vecchia zona ospitata.

   b. Nel pannello di navigazione, scegli Zone ospitate.

   c. Scegliere il nome della vecchia zona ospitata. Se hai molte zone ospitate, puoi scegliere Nome dominio esatto e immettere il nome della zona ospitata, quindi premere Invio per filtrare l'elenco.

   d. Se la zona ospitata contiene record diversi da quelli NS e SOA di default (ad esempio record alias che instradano il traffico verso un'istanza di policy di traffico), scegli la casella di controllo corrispondente e seleziona Elimina.

   e. Nel pannello di navigazione, scegli Zone ospitate.

f. Nell'elenco delle zone ospitate, scegliere il pulsante di opzione per la zona ospitata che si desidera eliminare.

g. Scegli Delete (Elimina).

Utilizzo dei record

Dopo aver creato una zona ospitata per il tuo dominio (come esempio.com), quindi crea record per indicare al Domain Name System (DNS) come desideri instradare il traffico su Internet per quel dominio.

Ad esempio, puoi creare record che fanno in modo che il DNS effettui le seguenti azioni:

- Instradare il traffico Internet per esempio.com all'indirizzo IP di un host nel tuo data center.
- Instradare le e-mail per quel dominio (ichiro@esempio.com) a un server e-mail (mail.esempio.com).
- Instradare il traffico per un sottodominio chiamato operations.tokyo.esempio.com all'indirizzo IP di un altro host.

Ogni record include il nome di un dominio o sottodominio, un tipo di record (ad esempio, un record con un tipo di MX instrada le e-mail) e altre informazioni applicabili al tipo di record (per i record MX, il nome host di uno o più server di posta e una priorità per ogni server). Per ulteriori informazioni sui diversi tipi di record, consulta Tipi di record DNS supportati.

Il nome di ciascun record in una zona ospitata deve terminare con il nome della zona ospitata. Ad esempio, la zona ospitata esempio.com può contenere record per i sottodomini www.esempio.com e accounting.tokyo.esempio.com, ma non può contenere record per un sottodominio www.esempio.ca.

> **Note**
>
> Per creare record per configurazioni di routing complesse, puoi usare il l'editor visivo del flusso di traffico e salvare la configurazione come una policy di traffico. Puoi quindi associare la policy di traffico a uno o più nomi di dominio (ad esempio esempio.com) o nomi di sottodominio (ad esempio www.esempio.com), nella stessa zona ospitata o in più zone ospitate. Inoltre, puoi eseguire il roll back degli aggiornamenti se la nuova configurazione non offre le prestazioni previste. Per ulteriori informazioni, consulta Utilizzo di Traffic Flow per instradare il traffico DNS.

Amazon Route 53 non prevede costi per i record che aggiungi a una zona ospitata. Per informazioni sul numero massimo di record che puoi creare in una zona ospitata, consulta Quote.

Argomenti

Scegliere una policy di routing

Quando crei un record, puoi scegliere una policy di routing che determina come Amazon Route 53 risponde alle query:

- Policy di routing semplice: utilizza questa opzione per una singola risorsa che esegue una determinata funzione per il tuo dominio, ad esempio un server Web che fornisce i contenuti per il sito Web esempio.com. Puoi utilizzare un routing semplice per creare i record in una zona ospitata privata.
- Policy di routing di failover: utilizza questa opzione se desideri configurare un failover attivo-passivo. Puoi utilizzare il routing di failover per creare i record in una zona ospitata privata.
- Policy di routing di geolocalizzazione: utilizza questa opzione se desideri instradare il traffico alle tue risorse in base alla posizione degli utenti. Puoi utilizzare il routing di geolocalizzazione per creare i record in una zona ospitata privata.
- Policy di routing di geoprossimità: utilizza questa opzione se desideri instradare il traffico in base alla posizione delle tue risorse e, facoltativamente, spostare il traffico dalle risorse in una posizione alle risorse in un'altra posizione. È possibile utilizzare il routing di geoprossimità per creare record in una zona ospitata privata.

- Politica di routing della latenza: utilizzala quando hai più risorse Regioni AWS e desideri indirizzare il traffico verso la regione che offre la latenza migliore. Puoi utilizzare il routing della latenza per creare i record in una zona ospitata privata.
- Policy di routing basato su IP: utilizza questa opzione quando desideri instradare il traffico in base alle posizioni degli utenti e disporre degli indirizzi IP da cui proviene il traffico.
- Policy di routing con risposta multivalore: utilizza questa opzione se desideri che Route 53 risponda alle query DNS con un massimo di otto record integri selezionati casualmente. Puoi utilizzare il routing di risposta multivalore per creare i record in una zona ospitata privata.
- Policy di routing ponderata: utilizza questa opzione se desideri instradare il traffico a più risorse nelle proporzioni specificate. Puoi utilizzare il routing ponderato per creare i record in una zona ospitata privata.

Argomenti

Routing semplice

Il routing semplice consente di configurare record DNS standard, senza un routing di Route 53 speciale, ad esempio ponderato o latenza. Con il routing semplice, in genere il traffico viene instradato a un'unica risorsa, ad esempio a un server Web per il tuo sito Web.

Puoi utilizzare una policy di instradamento semplice per creare i record in una zona ospitata privata.

Se scegli la policy di routing semplice nella console Route 53, non è possibile creare più record con lo stesso nome e tipo, ma è possibile specificare più valori nello stesso record, ad esempio più indirizzi IP. (Se scegli la politica di routing semplice per un record di alias, puoi specificare solo una

AWS risorsa o un record nella zona ospitata corrente.) Se specifichi più valori in un record, Route 53 restituisce tutti i valori al resolver ricorsivo in ordine casuale e il resolver restituisce i valori al client (ad esempio un browser Web) che ha inviato la query DNS. Il client, quindi, seleziona un valore e inoltra nuovamente la query. Con una policy di instradamento semplice è possibile specificare più indirizzi IP, ma su questi non viene eseguito alcun controllo dell'integrità.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing semplice per creare record, vedere i seguenti argomenti:

- Valori specifici per record semplici
- Valori specifici per record alias semplici
- Valori comuni per tutte le policy di routing
- Valori comuni per i record alias per tutte le policy di routing

Routing di failover

Il routing di failover consente di instradare il traffico verso una risorsa quando la risorsa è integra o a un'altra risorsa quando la prima risorsa non è integra. I record primari e secondari possono instradare il traffico verso qualsiasi risorsa da un bucket Amazon S3 configurato come sito Web in una complessa struttura di record. Per ulteriori informazioni, consulta Failover attivo-passivo.

Puoi utilizzare una policy di instradamento di failover per creare i record in una zona ospitata privata.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing del failover semplice per creare record, vedere i seguenti argomenti:

- Valori specifici per record di failover
- Valori specifici per i record alias di failover
- Valori comuni per tutte le policy di routing
- Valori comuni per i record alias per tutte le policy di routing

Routing di geolocalizzazione

Il routing di geolocalizzazione ti consente di scegliere le risorse in grado di gestire il traffico in base alla posizione geografica dei tuoi utenti, ossia la posizione da cui provengono le query DNS. È possibile, ad esempio, instradare tutte le query dall'Europa a un sistema di bilanciamento del carico Elastic Load Balancing nella regione di Francoforte.

Quando usi il routing di geolocalizzazione, puoi localizzare i tuoi contenuti e presentare alcuni o tutti i tuoi siti Web nel linguaggio dei tuoi utenti. Puoi utilizzare il routing di geolocalizzazione anche per limitare la distribuzione di contenuti solo ai percorsi in cui disponi di diritti di distribuzione. Un altro possibile utilizzo è quello di bilanciare il carico tra gli endpoint in modo prevedibile, in easy-to-manage modo che ogni posizione dell'utente venga indirizzata in modo coerente allo stesso endpoint.

Puoi specificare aree geografiche per continente, paese o stato degli Stati Uniti. Se crei record separati per regioni geografiche che si sovrappongono, ad esempio, un record per Nord America e uno per Canada, la priorità va alla regione geografica più piccola. In questo modo puoi instradare alcune query per un continente a una risorsa e instradare le query per determinati paesi su questo continente a un'altra risorsa. (Per un elenco di paesi in ciascun continente, consulta Ubicazione.)

La geolocalizzazione funziona attraverso la mappatura di indirizzi IP alle posizioni. Tuttavia, alcuni indirizzi IP non sono mappati ad aree geografiche, quindi anche se crei record di geolocalizzazione che coprono tutti i sette continenti, Amazon Route 53 riceverà alcune query DNS da posizioni che non è in grado di identificare. Puoi creare un record di default che gestisce le query da parte di indirizzi IP che non vengono mappati ad alcuna posizione e le query che provengono da posizioni per cui non hai creato record di geolocalizzazione. Se non crei un record di default, Route 53 restituisce "nessuna risposta" per le query provenienti da tali posizioni.

Puoi utilizzare una policy di instradamento basato sulla geolocalizzazione per creare i record in una zona ospitata privata o pubblica.

Per ulteriori informazioni, consulta Come Amazon Route 53 utilizza EDNS0 per stimare la posizione di un utente.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing di geolocalizzazione per creare record, vedere i seguenti argomenti:

- Valori specifici per record di geolocalizzazione
- Valori specifici per record degli alias di geolocalizzazione
- Valori comuni per tutte le policy di routing
- Valori comuni per i record alias per tutte le policy di routing

Instradamento della geolocalizzazione in zone ospitate privata

Per le zone ospitate private, Route 53 risponde alle query DNS in base al VPC da cui proviene Regione AWS la query. Per l'elenco di Regioni AWS, consulta Regioni e zone nella guida per EC2 l'utente di Amazon.

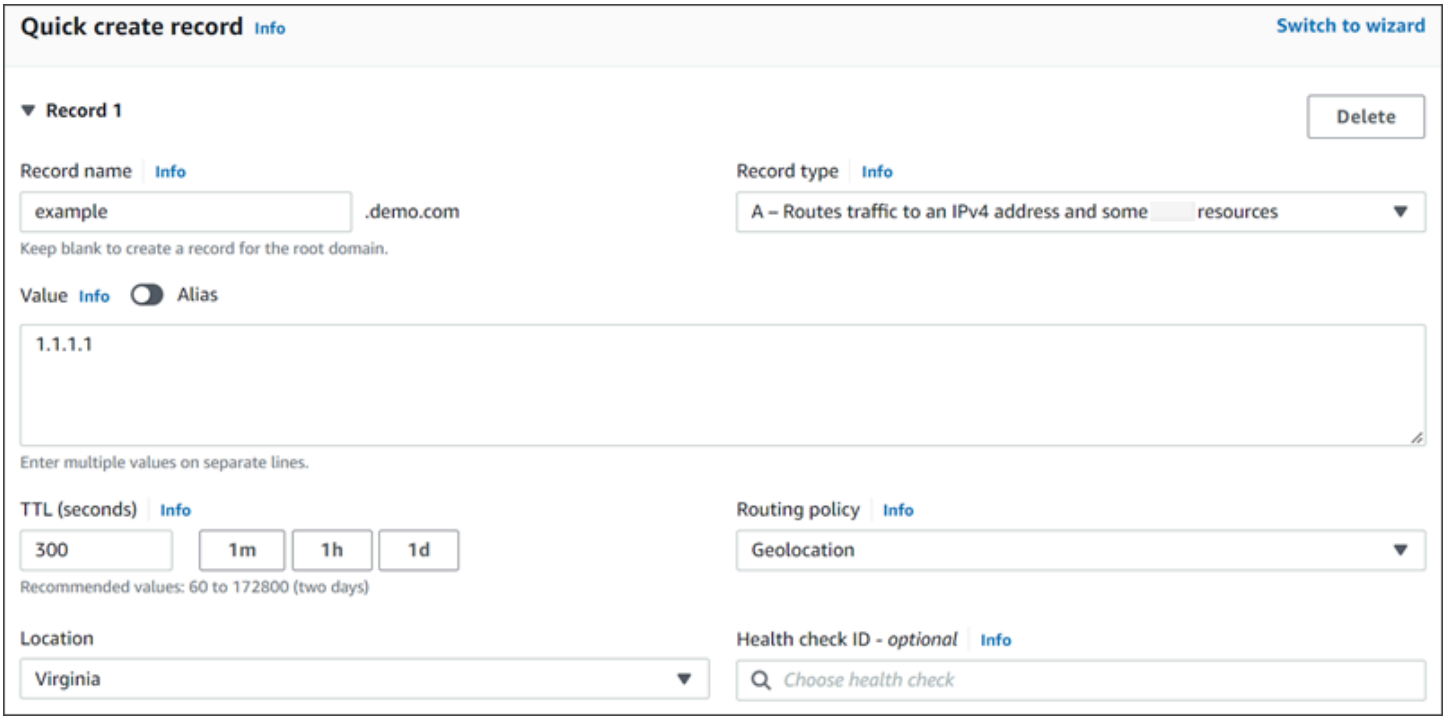
Se la query DNS proviene da una parte on-premise di una rete ibrida, verrà considerata come originata dal Regione AWS in cui si trova il VPC.

Se si includono controlli dell'integrità, è possibile creare record predefiniti per:

- Indirizzi IP che non sono mappati a posizioni geografiche.
- Query DNS provenienti da posizioni per le quali non hai creato record di geolocalizzazione.

Se il record di geolocalizzazione per la regione della query DNS non è integro, verrà restituito il record predefinito (se è integro).

Nella configurazione di esempio nella figura seguente, le query DNS provenienti da un us-east-1 Regione AWS (Virginia) verranno instradate all'endpoint 1.1.1.1.



Routing di geoprossimità

Il routing di geoprossimità consente ad Amazon Route 53 di instradare il traffico verso le tue risorse in base all'ubicazione geografica dei tuoi utenti e risorse. Indirizza il traffico verso la risorsa più vicina disponibile. Puoi anche scegliere di instradare più o meno traffico a una determinata risorsa specificando un valore, noto come bias. Un bias espande o restringe le dimensioni della regione geografica da cui il traffico viene instradato a una risorsa.

Puoi creare regole di geoprossimità per le tue risorse e specificare uno dei seguenti valori per ciascuna regola:

- Se utilizzi AWS risorse, specifica il gruppo Regione AWS di zone locali in cui hai creato la risorsa.
- Se non utilizzi AWS risorse, specifica la latitudine e la longitudine della risorsa.

Per utilizzare AWS Local Zones, devi prima abilitarle. Per ulteriori informazioni, consulta Nozioni di base sulle zone locali nella Guida per l'utente delle zone locali AWS .

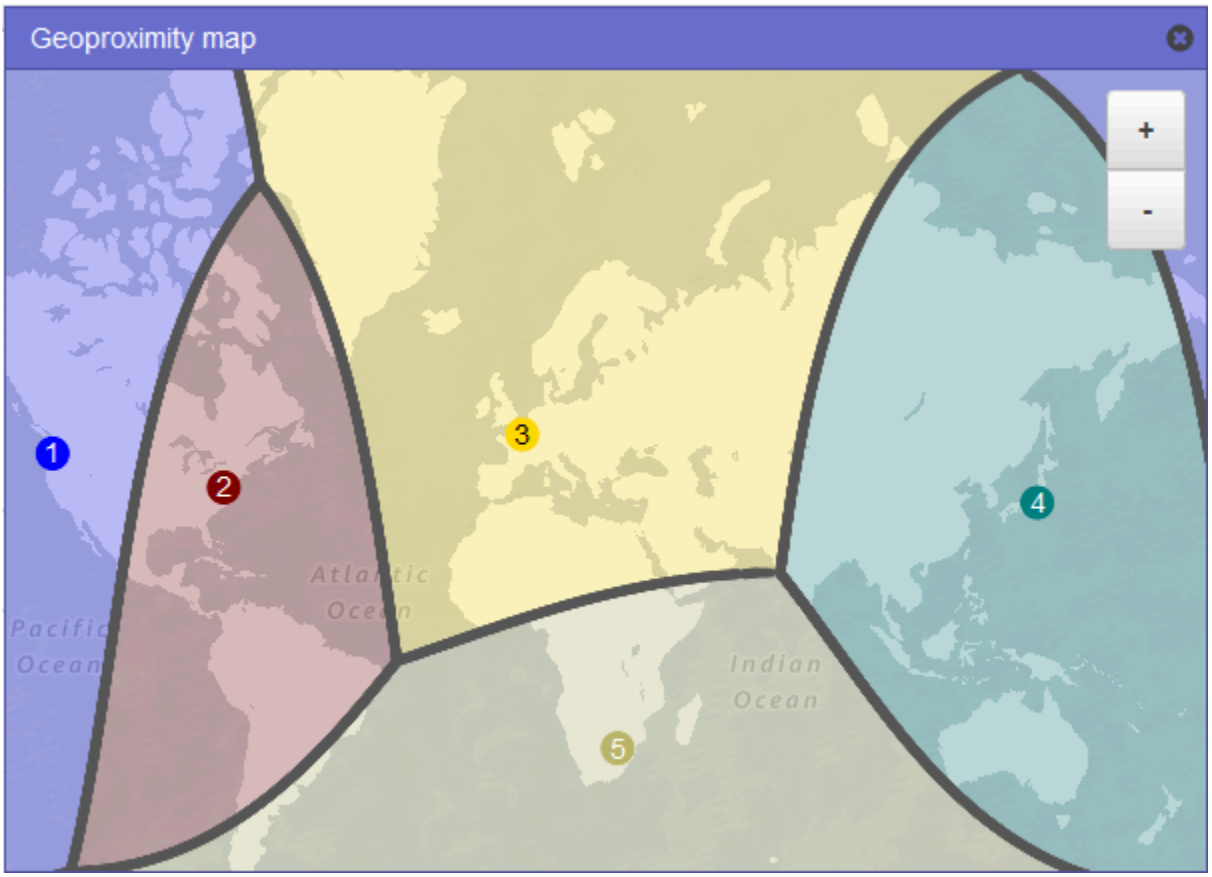
Per conoscere la differenza tra Regioni AWS e Local Zones, consulta Regions and Zones nella Amazon EC2 User Guide.

Per modificare facoltativamente le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica il valore applicabile per il bias:

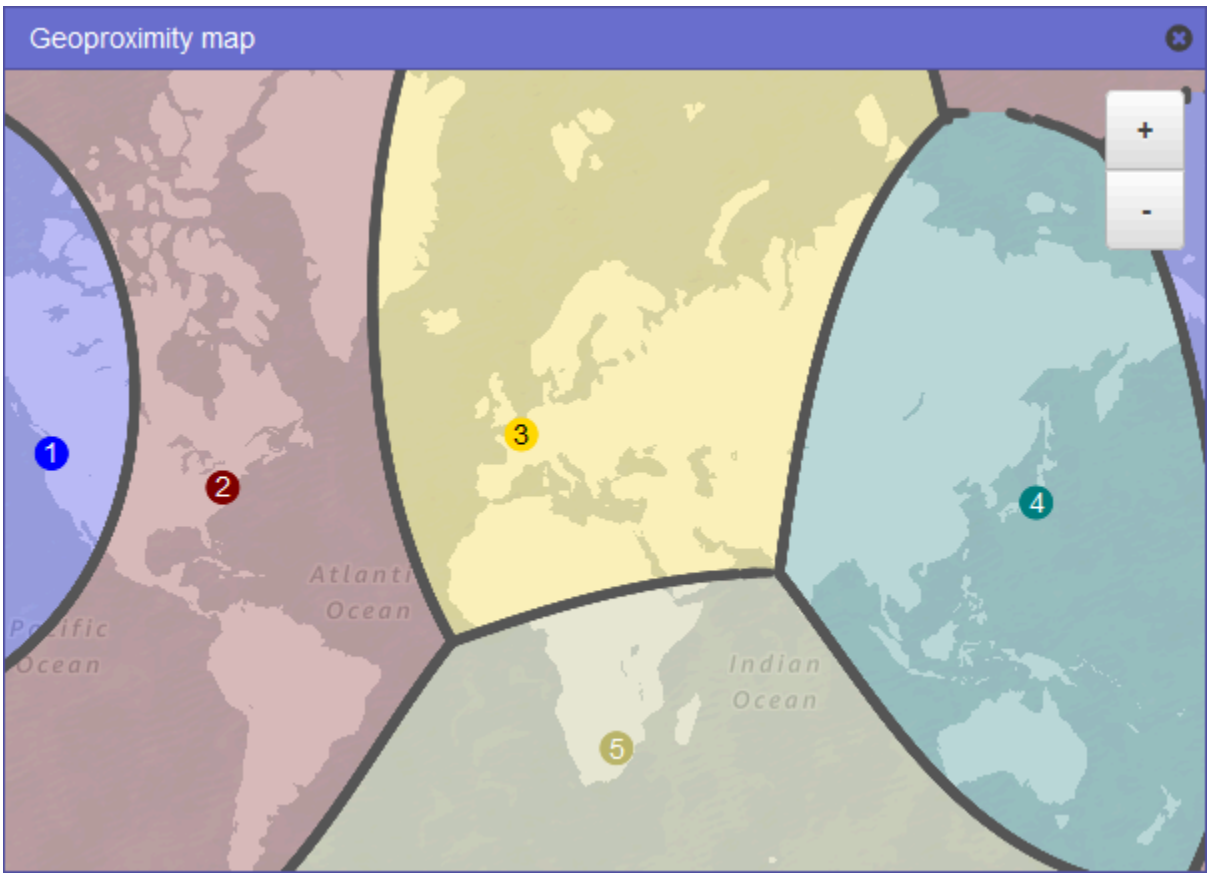
- Per espandere le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica un numero intero positivo tra 1 e 99 per il bias. Route 53 riduce le dimensioni delle regioni adiacenti.
- Per ridurre le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica un numero negativo tra -1 e -99 per il bias. Route 53 espande le dimensioni delle regioni adiacenti.

La mappa seguente ne mostra quattro Regioni AWS (numerati da 1 a 4) e una località a Johannesburg, in Sudafrica, specificata da latitudine e longitudine (5).

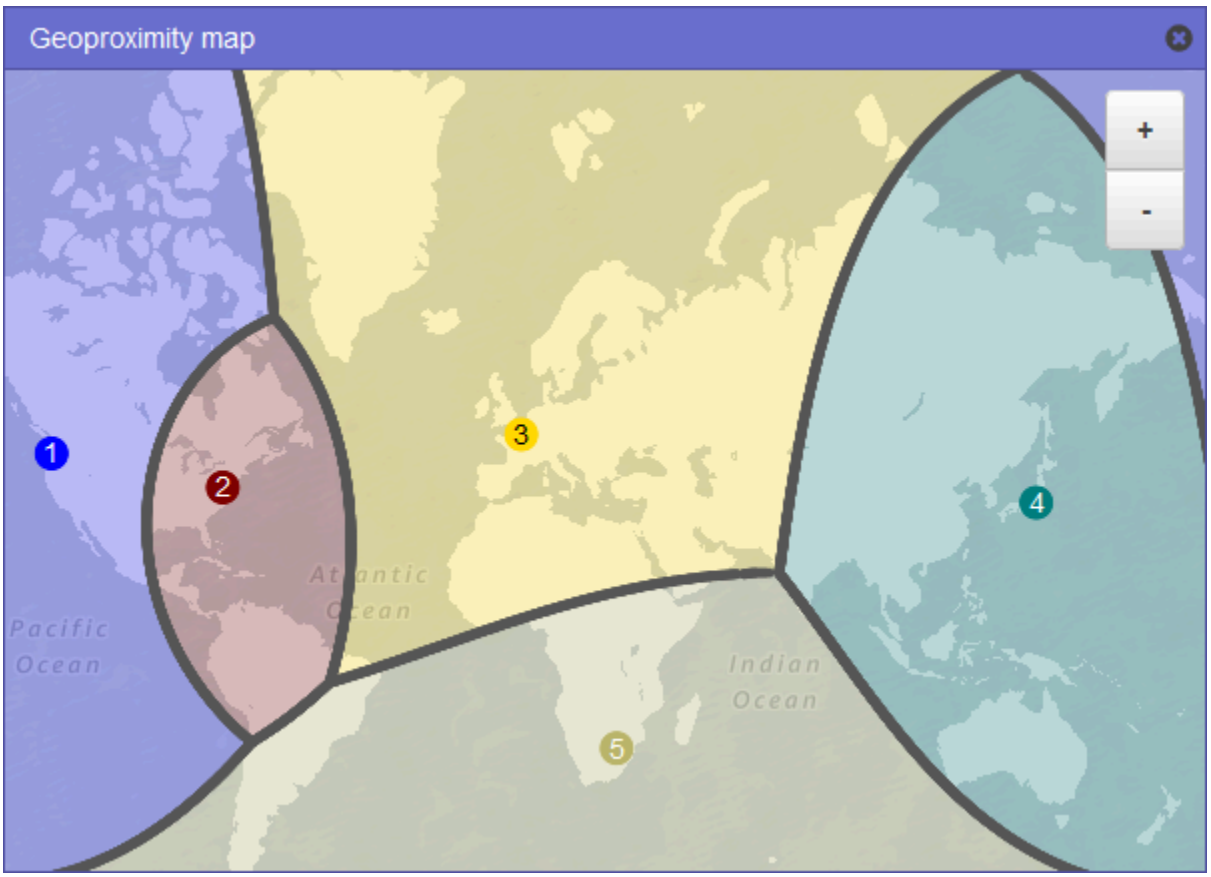
> **Note**
>
> Le mappe sono disponibili solo con il flusso di traffico.



La mappa seguente mostra cosa accade se si aggiunge un bias di +25 per la regione Stati Uniti orientali (Virginia settentrionale), numero 2 sulla mappa. Il traffico viene instradato alla risorsa in quella regione da una maggiore porzione di Nord America rispetto al passato e da tutto il Sud America.



La mappa seguente mostra cosa accade se si modifica il bias di -25 per la regione Stati Uniti orientali (Virginia settentrionale). Il traffico viene instradato alla risorsa in quella regione da una porzione minore rispetto al passato di Nord e Sud America e molto altro traffico viene instradato a risorse nelle regioni adiacenti 1, 3 e 5.



L'effetto della modifica del bias per le tue risorse dipende da una serie di fattori, tra cui le seguenti:

- Il numero di risorse di cui disponi.
- La vicinanza delle risorse tra loro.
- Il numero di utenti che hai vicino la zona di confine tra regioni geografiche. Ad esempio, supponiamo di avere risorse negli Regioni AWS Stati Uniti orientali (Virginia settentrionale) e negli Stati Uniti occidentali (Oregon) e di avere molti utenti a Dallas, Austin e San Antonio, Texas, USA. Queste città sono all'incirca equidistanti tra le risorse, quindi una piccola variazione di orientamento potrebbe comportare una forte oscillazione del traffico tra le risorse dell'una e l'altra. Regione AWS

È consigliabile modificare il bias in piccoli incrementi per evitare di sovraccaricare le risorse a causa di aumenti imprevisti del traffico.

Per ulteriori informazioni, consulta Come Amazon Route 53 utilizza EDNS0 per stimare la posizione di un utente.

Come Amazon Route 53 utilizza il bias per instradare il traffico

Ecco la formula che Amazon Route 53 utilizza per determinare come instradare il traffico:

Bias

```
Biased distance = actual distance * [1 - (bias/100)]
```

Quando il valore della distorsione è positivo, Route 53 considera l'origine di una query DNS e la risorsa specificata in un record di geoprossimità (EC2 ad esempio un'istanza in un Regione AWS) come se fossero più vicine tra loro di quanto non siano in realtà. Ad esempio, supponiamo che hai i seguenti record di geoprossimità:

- Un record per il server Web A, che dispone di un bias positivo di 50
- Un record per il server Web B, che non prevede alcun bias

Quando un record di geoprossimità dispone di un bias positivo di 50, Route 53 dimezza la distanza tra l'origine di una query e la risorsa per quel record. Route 53 calcola quindi la risorsa che è più vicina all'origine della query. Supponiamo che il server Web A è a 150 chilometri dall'origine di una query e il server Web B è a 100 chilometri. Se nessuno dei record ha un bias, Route 53 instrada le query al server Web B perché è più vicino. Tuttavia, poiché il record per il server Web A ha un bias positivo di 50, Route 53 tratta il server Web A come se fosse 75 chilometri dall'origine della query. Di conseguenza, Route 53 instrada le query al server Web A.

Ecco il calcolo per un bias positivo di 50:

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

Routing basato sulla latenza

Se la tua applicazione è ospitata su più server Regioni AWS, puoi migliorare le prestazioni degli utenti servendo le loro richieste da una piattaforma Regione AWS che offre la latenza più bassa.

> **Note**
>
> I dati sulla latenza tra gli utenti e le risorse si basano interamente sul traffico tra utenti e data center AWS . Se non utilizzi risorse in un ambiente Regione AWS, la latenza effettiva tra gli utenti e le tue risorse può variare in modo significativo rispetto ai dati di AWS latenza. Ciò vale anche se le risorse si trovano nella stessa città di una Regione AWS.

Per usare il routing basato sulla latenza, è necessario creare record di latenza per le risorse in più Regioni AWS. Quando Route 53 riceve una query DNS per il tuo dominio o sottodominio (esempio.com o acme.esempio.com), determina per quali Regioni AWS hai creato record di latenza, determina quale regione offre all'utente la latenza minima e quindi seleziona un record di latenza per quella regione. Route 53 risponde con il valore proveniente dal record selezionato, ad esempio l'indirizzo IP per un server Web.

Ad esempio, supponiamo di disporre di sistemi di bilanciamento del carico Elastic Load Balancing nella regione Stati Uniti occidentali (Oregon) e nella regione Asia Pacifico (Singapore). Crei un record di latenza per ogni sistema di bilanciamento del carico. Ecco cosa succede quando un utente a Londra immette il nome di dominio in un browser:

1. Il DNS instrada la query a un server dei nomi di Route 53.
2. Route 53 si riferisce ai propri dati sulla latenza tra Londra e la regione di Singapore e tra Londra e la regione dell'Oregon.
3. Se la latenza è inferiore tra le regioni di Londra e Oregon, Route 53 risponde alla query con l'indirizzo IP per il sistema di bilanciamento del carico dell'Oregon. Se la latenza è inferiore tra Londra e la regione di Singapore, Route 53 risponde con l'indirizzo IP per il sistema di bilanciamento del carico di Singapore.

La latenza tra host su Internet può cambiare nel tempo a causa delle modifiche di connettività di rete e di routing. Il routing basato sulla latenza si basa su misurazioni di latenza eseguite in un determinato periodo di tempo e le misurazioni rispecchiano queste modifiche. Una richiesta instradata alla regione dell'Oregon questa settimana potrebbe essere instradata alla regione di Singapore la prossima settimana.

> **Note**
>
> Quando un browser o un altro visualizzatore utilizza un resolver DNS che supporta l' edns-client-subnetestensione di EDNS0, il resolver DNS invia a Route 53 una versione troncata dell'indirizzo IP dell'utente. Se configuri il routing basato sulla latenza, Route 53 considera questo valore quando instrada il traffico alle tue risorse. Per ulteriori informazioni, consulta Come Amazon Route 53 utilizza EDNS0 per stimare la posizione di un utente.

Puoi utilizzare una policy di instradamento della latenza per creare i record in una zona ospitata privata.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing della latenza per creare record, vedere i seguenti argomenti:

- Valori specifici per i record di latenza
- Valori specifici per i record alias di latenza
- Valori comuni per tutte le policy di routing
- Valori comuni per i record alias per tutte le policy di routing

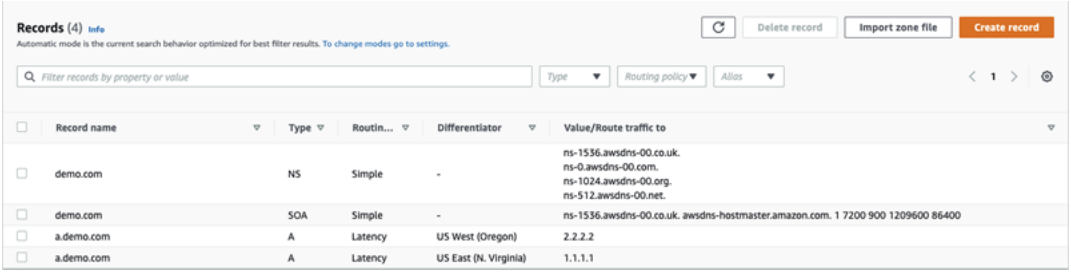
Instradamento basato sulla latenza in zone ospitate private

Per le zone ospitate private, Route 53 risponde alle query DNS con un endpoint che si trova nello stesso Regione AWS o è il più vicino in termini di distanza al VPC da cui ha avuto origine Regione AWS la query.

> **Note**
>
> Se hai un endpoint in uscita inoltrato a un endpoint in entrata, il record verrà risolto in base alla posizione dell'endpoint in entrata, non dell'endpoint in uscita.

Se si includono i controlli dell'integrità e il record con la latenza più bassa rispetto all'origine della query non è integro, viene restituito un endpoint integro con la successiva latenza più bassa.

Nella configurazione di esempio riportata nella figura seguente, le query DNS provenienti da un us-east-1 Regione AWS, o più vicino ad esso, verranno instradate all'endpoint 1.1.1.1. Le query DNS da us-west-2, o da regione vicina, verranno instradate all'endpoint 2.2.2.2.



Routing basato su IP

Con il routing basato su IP in Amazon Route 53, puoi ottimizzare il routing DNS sfruttando la tua comprensione della rete, delle applicazioni e dei client per prendere le migliori decisioni di routing DNS per gli utenti finali. Il routing basato su IP offre un controllo granulare per ottimizzare le prestazioni o ridurre i costi di rete caricando i dati su Route 53 sotto forma di mappature. user-IP-to-endpoint

I routing di geolocalizzazione e della latenza si basano sui dati che Route 53 raccoglie e mantiene aggiornati. Questo approccio funziona per la maggior parte dei clienti, ma il routing basato su IP offre la possibilità aggiuntiva di ottimizzare il routing a seconda delle conoscenze specifiche del tuo portafoglio clienti. Ad esempio, un provider globale di contenuti video potrebbe voler instradare gli utenti finali da un provider di servizi Internet (ISP) specifico.

Quelli che seguono sono alcuni dei casi di utilizzo più frequenti dell'instradamento basato su IP:

- Desideri indirizzare gli utenti finali da determinati endpoint a endpoint specifici ISPs in modo da ottimizzare i costi o le prestazioni del transito di rete.
- Desideri aggiungere delle sostituzioni ai tipi di instradamento di Route 53 esistenti, come l'instradamento basato sulla geolocalizzazione, sulla base della conoscenza delle posizioni fisiche dei clienti.

Gestione degli intervalli IP e loro associazione a un set di record di risorse () RRSet

Ad IPv4 esempio, è possibile utilizzare blocchi CIDR compresi tra 1 e 24 bit di lunghezza, inclusi, mentre perIPv6, è possibile utilizzare blocchi CIDR tra 1 e 48 bit di lunghezza, inclusi. Per definire un blocco CIDR a zero bit (0.0.0.0/0 o ::/0), utilizza la posizione predefinita ("*").

Per le query DNS con un CIDR più lungo di quello specificato nella raccolta CIDR, Route 53 lo abbinerà al CIDR più breve. Ad esempio, se specifichi 2001:0DB8: :/32 come blocco CIDR nella tua raccolta CIDR e una query ha origine da 2001:0:0000:1234: :/48, corrisponderà. DB8 Se, d'altra parte, specifichi 2001:0DB8: 0000:1234: :/48 nella tua raccolta CIDR e una query ha origine da

2001:0DB8: :/32, questa non corrisponderà e Route 53 risponderà con il record per la posizione predefinita («*»).

Puoi raggruppare i set di blocchi CIDR (o gli intervalli IP) in posizioni CIDR, che a loro volta sono raggruppate in entità riutilizzabili chiamate raccolte CIDR:

blocco CIDR

Un intervallo IP in notazione CIDR, ad esempio 192.0.2.0/24 o 2001:: :/32. DB8

Posizione CIDR

Un elenco con i nomi dei blocchi CIDR. Ad esempio, example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:: :/32]. DB8 I blocchi in un elenco di posizioni CIDR non devono essere adiacenti o avere lo stesso intervallo.

Una singola posizione può avere entrambi i blocchi e questa posizione può essere associata rispettivamente ai set di record A e AAAA. IPv4 IPv6

Per convenzione, di solito il nome è una posizione, ma può essere qualsiasi stringa, ad esempio Company-A.

Raccolta CIDR

Una raccolta con i nomi delle posizioni. Ad esempio, mycollection = [example-isp-seattle, example-isp-tokyo].

I set del record della risorsa di routing basato su IP fanno riferimento a una posizione in una raccolta e tutti i set del record della risorsa per lo stesso nome e tipo di set devono fare riferimento alla stessa raccolta. Ad esempio, se crei siti Web in due regioni e desideri indirizzare le query DNS da due diverse posizioni CIDR verso un sito Web specifico in base agli indirizzi IP di origine, entrambe le posizioni devono essere elencate nella stessa raccolta CIDR.

Puoi utilizzare una policy di instradamento basato su IP per creare i record in una zona ospitata privata.

Per ulteriori informazioni sui valori specificati dall'utente quando utilizzi la policy di routing basato su IP per creare i record, consulta i seguenti argomenti:

- Valori specifici per i record basati su IP
- Valori specifici per i record alias basati su IP
- Valori comuni per tutte le policy di routing

- Valori comuni per i record alias per tutte le policy di routing

Argomenti

- Creazione di una raccolta CIDR con posizioni e blocchi CIDR
- Utilizzo di posizioni e blocchi CIDR
- Eliminazione di una raccolta CIDR
- Spostamento di una geolocalizzazione in un routing basato su IP

Creazione di una raccolta CIDR con posizioni e blocchi CIDR

Per iniziare, crea una raccolta CIDR e aggiungi i blocchi e le posizioni CIDR.

Creazione di una raccolta CIDR tramite la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli IP-based routing (Routing basato su IP), quindi CIDR collections (Raccolte CIDR).
3. Seleziona Create CIDR collection (Crea raccolta CIDR).
4. Nel riquadro Create CIDR collection (Crea raccolta CIDR), in Details (Dettagli), inserisci un nome per la raccolta.
5. Scegli Create collection (Crea raccolta) per creare una raccolta vuota.

   oppure

   Nella sezione Crea posizioni CIDR, inserisci un nome per la posizione CIDR nella casella Posizione CIDR. Il nome della posizione può essere una qualsiasi stringa identificativa, ad esempio **`company 1`** o **`Seattle`**. Non deve essere obbligatoriamente una posizione geografica effettiva.

   > **Important**
   >
   > Il nome della posizione CIDR ha una lunghezza massima di 16 caratteri.

Inserisci i blocchi CIDR nella casella Blocchi CIDR, uno per riga. Questi possono essere IPv4 IPv6 indirizzi che vanno da /0 a /24 per IPv4 e da /0 a /48 per. IPv6

6. Dopo avere inserito i blocchi CIDR, scegli Create CIDR collection (Crea raccolta CIDR) oppure Add another location (Aggiungi un'altra posizione) per continuare a inserire le posizioni e il blocco CIDR. Puoi inserire più posizioni CIDR per raccolta.
7. Dopo avere inserito le posizioni CIDR, scegli Create CIDR collection (Crea raccolta CIDR).

Utilizzo di posizioni e blocchi CIDR

Utilizzo delle posizioni CIDR tramite la console Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, scegli IP-based routing (Routing basato su IP), CIDR collections (Raccolte CIDR) e poi, nella sezione CIDR collections (Raccolte CIDR), fai clic su un collegamento a una raccolta CIDR nell'elenco Collection name (Nome raccolta).

   Nella pagina CIDR locations (Posizioni CIDR), puoi creare, eliminare o modificare una posizione CIDR e i relativi blocchi.

   - Per creare una posizione, scegli Create CIDR location (Crea posizione CIDR).
   - Nel riquadro Create CIDR location (Crea posizione CIDR), inserisci un nome per la posizione e i blocchi CIDR associati a essa, quindi scegli Create (Crea).
   - Per visualizzare una posizione CIDR e i blocchi al suo interno, scegli il pulsante di opzione accanto a una posizione per mostrare il nome e i blocchi CIDR nel riquadro della posizione.

     In questo riquadro puoi anche scegliere Modifica per aggiornare il nome della posizione o i suoi blocchi CIDR. Scegli Salva una volta completata la modifica.
   - Per eliminare una posizione CIDR e i blocchi al suo interno, scegli il pulsante di opzione accanto alla posizione che desideri eliminare, quindi seleziona Delete (Elimina). Per confermare l'eliminazione, inserisci il nome della posizione nel campo di immissione del testo e scegli di nuovo Delete (Elimina).

> **Important**
>
> L'eliminazione di una posizione CIDR non può essere annullata. Se hai dei record DNS associati alla posizione, il tuo dominio potrebbe diventare irraggiungibile.

Eliminazione di una raccolta CIDR

Eliminazione di una raccolta CIDR, le relative posizioni e i blocchi tramite la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli IP-based routing (Routing basato su IP) quindi CIDR collections (Raccolte CIDR).
3. Nella sezione CIDR collections (Raccolte CIDR), fai clic sul nome collegato della raccolta che desideri eliminare.
4. Nella pagina CIDR locations (Posizioni CIDR), seleziona ogni posizione una alla volta, scegli Delete (Elimina), inserisci il nome nella finestra di dialogo, quindi scegli Delete (Elimina). Prima di eliminare la raccolta, devi eliminare ogni posizione associata a una raccolta CIDR.
5. Al termine dell'eliminazione di ogni posizione CIDR, nella pagina CIDR locations (Posizioni CIDR) scegli il pulsante di opzione accanto alla raccolta che desideri eliminare, quindi seleziona Delete (Elimina).

Spostamento di una geolocalizzazione in un routing basato su IP

Se utilizzi le policy di routing di geolocalizzazione o geoprossimità e visualizzi costantemente client specifici instradati a un endpoint che non è ottimale in base alla loro posizione fisica o alla topologia di rete, puoi indirizzare meglio gli intervalli IP pubblici di questi client utilizzando il routing basato su IP.

La tabella seguente contiene un esempio di configurazione della geolocalizzazione per un routing di geolocalizzazione esistente che ottimizzeremo per gli intervalli IP della California.

Nome del set del record	Policy di routing e origine	Indirizzo IP dell'endpoint dell'applicazione

Nome del set del record	Policy di routing e origine	Indirizzo IP dell'endpoint dell'applicazione
esempio.com	Routing di geolocalizzazione (Stati uniti)	`198.51.100.1`
esempio.com	Routing di geolocalizzazione (UE)	`198.51.100.2`

Per sostituire gli intervalli IP dalla California e passare a un nuovo endpoint dell'applicazione, ricrea innanzitutto il routing di geolocalizzazione con un nuovo nome del set del record.

Nome del set del record	Policy di routing e origine	Indirizzo IP dell'endpoint dell'applicazione
geo.esempio.com	Routing di geolocalizzazione (Stati uniti)	`198.51.100.1`
geo.esempio.com	Routing di geolocalizzazione (UE)	`198.51.100.2`

Quindi, crea i record di routing basati su IP e un record predefinito che punta al recordset di routing di geolocalizzazione ricreato recentemente.

Nome del set del record	Policy di routing e origine	Indirizzo IP dell'endpoint dell'applicazione
esempio.com	Routing basato su IP (predefinito)	Record alias per l'endpoint dell'applicazione geo.esempio.com che desideri come predefinito. Ad esempio `198.51.100.1` .

Nome del set del record	Policy di routing e origine	Indirizzo IP dell'endpoint dell'applicazione
esempio.com	Routing basato su IP (intervalli IP della California)	`198.51.100.3`

Routing di risposta multivalore

Il routing con risposta multivalore ti consente di configurare Amazon Route 53 per restituire più valori, ad esempio indirizzi IP per i server Web, in risposta alle query DNS. Puoi specificare più valori per quasi tutti i record, ma il routing di risposta multivalore ti consente di controllare lo stato di ciascuna risorsa, perciò Route 53 restituisce valori solo per le risorse integre. Non è un sostituito per un load balancer, ma la capacità di restituire indirizzi IP multipli il cui stato può essere controllato è un modo per utilizzare il DNS al fine di migliorare capacità e load balancer.

Per instradare il traffico in modo casuale a più risorse, ad esempio server Web, devi creare un record di risposta multivalore per ciascuna risorsa e, facoltativamente, associare un controllo dell'integrità di Route 53 a ogni record. Route 53 risponde alle query DNS con un massimo di otto record integri e offre diverse risposte a diversi resolver DNS. Se un server Web non è più disponibile dopo che un resolver memorizza una risposta nella cache, il software client può provare un altro indirizzo IP nella risposta.

Tieni presente quanto segue:

- Se associ un controllo dell'integrità a un record di risposta multivalore, Route 53 risponde alle query DNS con l'indirizzo IP corrispondente solo quando il controllo dell'integrità è positivo.
- Se non associ un controllo dell'integrità a un record di risposta multivalore, Route 53 considera sempre il record come integro.
- Se disponi di otto o meno record integri, Route 53 risponde alle query DNS con tutti i record integri.
- Quando tutti i record non sono integri, Route 53 risponde alle query DNS con un massimo di otto record non integri.

Puoi utilizzare una policy di instradamento con risposta multivalore per creare i record in una zona ospitata privata.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing di risposta multivalore per creare record, vedere Valori specifici per record di risposta multivalore e Valori comuni per tutte le policy di routing.

Routing ponderato

Il routing ponderato consente di associare più risorse con un solo nome di dominio (esempio.com) o nome di sottodominio (acme.esempio.com) e di scegliere la quantità di traffico che viene instradato a ciascuna risorsa. Questo può essere utile per un'ampia gamma di scopi, tra cui il bilanciamento del carico e il test di nuove versioni di software.

Per configurare il routing ponderato, devi creare record con lo stesso nome e tipo per ciascuna delle tue risorse. Puoi assegnare a ogni record un peso relativo che corrisponde alla quantità di traffico che desideri inviare a ogni risorsa. Amazon Route 53 invia il traffico a una risorsa in base al peso che assegni al record come proporzione del peso totale per tutti i record nel gruppo:

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Ad esempio, se desideri inviare una piccola porzione di traffico a una risorsa e il resto a un'altra risorsa, devi specificare un peso di 1 e 255. La risorsa con un peso pari a 1 ottiene 1/256esimo del traffico (01/(01+255)) e l'altra risorsa ottiene 255/256esimi (255/(1+255)). Puoi modificare gradualmente il carico modificando i pesi. Se desideri interrompere l'invio del traffico a una risorsa, puoi modificare il peso per quel record su 0.

Per ulteriori informazioni sui valori specificati dall'utente quando si utilizza la policy di routing ponderato per creare record, vedere i seguenti argomenti:

- Valori specifici per record ponderati
- Valori specifici per i record alias ponderati
- Valori comuni per tutte le policy di routing
- Valori comuni per i record alias per tutte le policy di routing

Puoi utilizzare una policy di instradamento ponderato per creare i record in una zona ospitata privata.

Controlli dell'integrità e routing ponderato

Se aggiungi controlli dell'integrità a tutti i record di un gruppo di record ponderati, ma ad alcuni record assegni un peso diverso da zero e ad altri un peso pari a zero, i controlli dell'integrità funzionano come se tutti i record avessero un peso diverso da zero, con le seguenti eccezioni:

- Route 53 inizialmente considera solo i record ponderati diversi da zero, se esistenti.
- Se tutti i record con un peso maggiore di 0 non sono integri, allora Route 53 considera i record con peso zero.

La tabella seguente descrive il comportamento previsto quando il record con peso 0 comprende un controllo dell'integrità:

	Record 1	Record 2	Record 3
Weight	1	1	0
Comprende un controllo dell'integrità?	Sì	Sì	Sì
Stato del controllo dell'integrità	Non integro	Non integro	Integro
Si è ricevuta una risposta alla query DNS?	No	No	Sì
Stato del controllo dell'integrità	Non integro	Non integro	Non integro
Si è ricevuta una risposta alla query DNS?	Sì	Sì	No
Stato del controllo dell'integrità	Non integro	Integro	Non integro
	No	Sì	No

	Record 1	Record 2	Record 3
Si è ricevuta una risposta alla query DNS?			
Stato del controllo dell'integrità	Integro	Integro	Non integro
Si è ricevuta una risposta alla query DNS?	Sì	Sì	No
Stato del controllo dell'integrità	Integro	Integro	Integro
Si è ricevuta una risposta alla query DNS?	Sì	Sì	No

La tabella seguente descrive il comportamento previsto quando il record con peso 0 non comprende un controllo dell'integrità:

	Record 1	Record 2	Record 3
Weight	1	1	0
Comprende un controllo dell'integrità?	Sì	Sì	No
Stato del controllo dell'integrità	Integro	Integro	N/D

	Record 1	Record 2	Record 3
Si è ricevuta una risposta alla query DNS?	Sì	Sì	No
Stato del controllo dell'integrità	Non integro	Non integro	N/D
Si è ricevuta una risposta alla query DNS?	No	No	Sì
Stato del controllo dell'integrità	Non integro	Integro	N/D
Si è ricevuta una risposta alla query DNS?	No	Sì	No

Come Amazon Route 53 utilizza EDNS0 per stimare la posizione di un utente

Per migliorare la precisione di geolocalizzazione, geoprossimità, routing basato su IP e latenza, Amazon Route 53 supporta l'estensione di EDNS0. edns-client-subnet (EDNS0 aggiunge diverse estensioni facoltative al protocollo DNS). Route 53 può essere utilizzato solo quando i resolver DNS lo supportano: edns-client-subnet

- Quando un browser o un altro visualizzatore utilizza un resolver DNS che non supporta edns-client-subnet, Route 53 utilizza l'indirizzo IP di origine del resolver DNS per approssimare la posizione dell'utente e risponde alle query di geolocalizzazione con il record DNS relativo alla posizione del resolver.
- Quando un browser o un altro visualizzatore utilizza un resolver DNS che lo supporta edns-client-subnet, il resolver DNS invia a Route 53 una versione troncata dell'indirizzo IP dell'utente. Route 53 determina la posizione dell'utente in base all'indirizzo IP troncato anziché l'indirizzo IP di origine

dell'autore della resolver DNS; questo normalmente fornisce una stima più precisa sulla posizione dell'utente. Route 53 risponde quindi alle query di geolocalizzazione con il record DNS per la posizione dell'utente.

- EDNS0 non è applicabile alle zone ospitate private. Per le zone ospitate private, Route 53 utilizza i dati dei Resolver Route 53 in cui si trova la zona ospitata privata per prendere decisioni sulla geolocalizzazione e sul Regione AWS routing della latenza.

Per ulteriori informazioni su edns-client-subnet, consulta EDNS Client Subnet RFC, Client Subnet in DNS Requests.

Scelta tra record alias e non alias

I record alias di Amazon Route 53 forniscono un'estensione specifica di Route 53 alla funzionalità DNS. I record di alias consentono di indirizzare il traffico verso AWS risorse selezionate, tra cui, a titolo esemplificativo, CloudFront distribuzioni e bucket Amazon S3. Inoltre, consentono di instradare il traffico da un record in una zona ospitata a un altro record.

A differenza del record CNAME, puoi creare un record alias sul nodo superiore di uno spazio dei nomi DNS, noto anche come apex di zona. Ad esempio, se record il nome DNS esempio.com, l'apex di zona è esempio.com. Non puoi creare un record CNAME per esempio.com, ma puoi creare un record alias per esempio.com che esegue l'instradamento del traffico in www.esempio.com (purché il tipo di record per www.esempio.com non sia già CNAME).

Quando Route 53 riceve una query DNS per un record alias, Route 53 risponde con il valore applicabile per la risorsa:

- Un'API regionale personalizzata di Amazon API Gateway o un'API ottimizzata per l'edge: Route 53 risponderà con uno o più indirizzi IP per l'API.
- Un endpoint dell'interfaccia Amazon VPC: Route 53 risponderà con uno o più indirizzi IP per l'endpoint dell'interfaccia.
- Una CloudFront distribuzione: Route 53 risponde con uno o più indirizzi IP per i server CloudFront edge che possono servire i tuoi contenuti.
- Servizio App Runner: Route 53 risponde con uno o più indirizzi IP.
- Un ambiente Elastic Beanstalk: Route 53 risponderà con uno o più indirizzi IP per l'ambiente.
- Un sistema di bilanciamento del carico Elastic Load Balancing: Route 53 risponde con uno o più indirizzi IP del sistema di bilanciamento del carico. Ciò include Application Load Balancer, Classic Load Balancer e Network Load Balancer.

- Un AWS Global Accelerator acceleratore: Route 53 risponde con gli indirizzi IP dell'acceleratore.
- Un OpenSearch servizio: Route 53 risponde con uno o più indirizzi IP per il dominio personalizzato del OpenSearch servizio.
- Un bucket Amazon S3 configurato come sito Web statico: Route 53 risponderà a ogni richiesta con un indirizzo IP per il bucket Amazon S3.
- Un altro record Route 53 dello stesso tipo nella stessa zona ospitata: Route 53 risponde come se la query fosse per il record a cui fa riferimento il record alias (consulta Confronto tra record alias e CNAME).
- AWS AppSync nome di dominio: Route 53 risponde con uno o più indirizzi IP per l'endpoint di interfaccia.

Per ulteriori informazioni, consulta Instradamento del traffico Internet verso le tue risorse AWS.

Quando si utilizza un record di alias per indirizzare il traffico verso una AWS risorsa, Route 53 riconosce automaticamente le modifiche nella risorsa. Ad esempio, supponiamo che un record alias di un example.com punti a un sistema di bilanciamento del carico Elastic Load Balancing presso lb1-1234.us-east-2.elb.amazonaws.com. Se l'indirizzo IP del load balancer cambia, Route 53 inizia a rispondere automaticamente alle query DNS utilizzando il nuovo indirizzo IP.

Se un record di alias punta a una AWS risorsa, non è possibile impostare il time to live (TTL); Route 53 utilizza il TTL predefinito per la risorsa. Se un record alias punta a un altro record nella stessa zona ospitata, Route 53 usa il TTL del record a cui punta il record alias. Per ulteriori informazioni sul valore TTL (Time to Live) corrente per Elastic Load Balancing, consulta Routing della richiesta nella Guida per l'utente di Elastic Load Balancing e cerca "ttl".

Per informazioni sulla creazione di record utilizzando la console Route 53, consulta Creazione di record utilizzando la console Amazon Route 53. Per informazioni sui valori che specifichi per i record alias applicabili, consulta l'argomento relativo in Di seguito sono descritti i valori che devi specificare durante la creazione o la modifica di record di Amazon Route 53.:

- Valori specifici per record alias semplici
- Valori specifici per i record alias ponderati
- Valori specifici per i record alias di latenza
- Valori specifici per i record alias di failover
- Valori specifici per record degli alias di geolocalizzazione

- Valori specifici per i record di alias di geoprossimità
- Valori comuni per i record alias per tutte le policy di routing

Confronto tra record alias e CNAME

I record alias sono simili a record CNAME, ma ci sono alcune differenze importanti. Nell'elenco seguente vengono confrontati i record alias e i record CNAME.

Risorse verso cui è possibile reindirizzare le query

Record alias

Un record di alias può reindirizzare le query solo a AWS risorse selezionate, tra cui, a titolo esemplificativo ma non esaustivo, quanto segue:

- Bucket Amazon S3
- CloudFront distribuzioni
- Un altro record nella stessa zona ospitata Route 53

Ad esempio, è possibile creare un record alias denominato acme.esempio.com che reindirizza le query a un bucket Amazon S3, anch'esso denominato acme.esempio.com. È anche possibile creare un record alias acme.esempio.com che reindirizza le query a un record denominato zenith.example.com nella zona ospitata esempio.com.

Registri CNAME

Un record CNAME può reindirizzare query DNS a qualsiasi record DNS. Ad esempio, è possibile creare un record CNAME che reindirizza le query da acme.esempio.com a zenith.example.com o ad acme.example.org. Non è necessario utilizzare Route 53 come servizio DNS per il dominio a cui si stanno reindirizzando le query.

Creazione di record con lo stesso nome del dominio (record all'apex di zona)

Record alias

Nella maggior parte delle configurazioni, è possibile creare un record alias con lo stesso nome della zona ospitata (apex di zona). L'unica eccezione è quando si desidera reindirizzare le query dall'apex di zona (come esempio.com) per un record nella stessa zona ospitata che dispone di un tipo CNAME (ad esempio zenith.esempio.com). Il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Registri CNAME

Non è possibile creare un record CNAME con lo stesso nome della zona ospitata (apex di zona). Questo vale sia per le zone ospitate che per i nomi di dominio (esempio.com) e per le zone ospitate dei sottodomini (zenith.esempio.com).

Prezzi per query DNS

Record alias

Route 53 non addebita alcun costo per le richieste di alias alle risorse. AWS Per ulteriori informazioni, consulta la pagina dei Prezzi Amazon Route 53.

Registri CNAME

Route 53 prevede addebiti per le query CNAME.

> **Note**
>
> Se crei un record CNAME che esegue il reindirizzamento al nome di un altro record in una zona ospitata Route 53 (la stessa zona ospitata o un'altra zona ospitata), ogni query DNS viene addebitata come due query:
>
> - Route 53 risponde alla prima query DNS con il nome del record verso cui eseguire il reindirizzamento.
> - Il resolver DNS deve quindi inviare un'altra query per il record nella prima risposta per ottenere informazioni su dove indirizzare il traffico, ad esempio l'indirizzo IP di un server Web.
>
> Se il record CNAME esegue il reindirizzamento al nome di un record ospitato con un altro servizio DNS, Route 53 addebita una query. L'altro servizio DNS potrebbe addebitare la seconda query.

Tipo di record specificato nella query DNS

Record alias

Route 53 risponde a una query DNS solo quando il nome del record alias (ad esempio acme.esempio.com) e il tipo di record alias (ad esempio A o AAAA) corrispondono al nome e al tipo della query DNS.

Registri CNAME

Un record CNAME esegue il reindirizzamento delle query DNS per un nome di record a prescindere dal tipo di record specificato nella query DNS, ad esempio A o AAAA.

Come vengono elencati i record nelle query dig o nslookup

Record alias

Nella risposta a una query dig o nslookup, un record alias viene elencato come il tipo di record specificato al momento della creazione del record, ad esempio A o AAAA. (Il tipo di record specificato per un record alias dipende dalla risorsa verso cui si sta instradando il traffico. Ad esempio, per instradare il traffico a un bucket S3, specifica A per il tipo.) La proprietà alias è visibile solo nella console Route 53 o nella risposta a una richiesta programmatica, ad esempio un comando CLI AWS . `list-resource-record-sets`

Registri CNAME

Un record CNAME viene elencato come un record CNAME in risposta alle query d'individuazione o di ricerca.

Tipi di record DNS supportati

Amazon Route 53 supporta i tipi di record DNS elencati in questa sezione. Ogni tipo di record include anche un esempio di come formattare l'elemento `Value` quando accedi a Route 53 utilizzando l'API.

> **Note**
>
> Per i tipi di record che includono un nome di dominio, immetto un nome di dominio completo, ad esempio, www.esempio.com. Il punto finale è facoltativo; Route 53 presuppone che il nome di dominio sia completo. Ciò significa che Route 53 considera identici www.esempio.com (senza un punto finale) e www.esempio.com. (con un punto finale).

Route 53 fornisce un'estensione alla funzionalità DNS nota come record alias. Analogamente ai record CNAME, i record alias consentono di indirizzare il traffico verso AWS risorse selezionate, come CloudFront distribuzioni e bucket Amazon S3. Per ulteriori informazioni, incluso un confronto tra record alias e CNAME, vedi Scelta tra record alias e non alias.

Argomenti

Tipo di record A

Utilizzi un record A per indirizzare il traffico verso una risorsa, ad esempio un server Web, utilizzando un IPv4 indirizzo in notazione decimale puntata.

Esempio per la console Amazon Route 53

```
192.0.2.1
```

Esempio per l'API Route 53

```
<Value>192.0.2.1</Value>
```

Tipo di record AAAA

Si utilizza un record AAAA per indirizzare il traffico verso una risorsa, ad esempio un server Web, utilizzando un IPv6 indirizzo in formato esadecimale separato da due punti.

Esempio per la console Amazon Route 53

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Esempio per l'API Route 53

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

Tipo di record CAA

Un record CAA specifica quali autorità di certificazione (CAs) sono autorizzate a emettere certificati per un dominio o sottodominio. La creazione di un record CAA aiuta a prevenire l'emissione errata di certificati per CAs i tuoi domini. Un record CAA non è un sostituto per i requisiti di sicurezza specificati dall'autorità di certificazione, ad esempio il requisito di convalidare che sei il proprietario di un dominio.

Puoi utilizzare i record CAA per specificare quanto segue:

- Quali autorità di certificazione (CAs) possono emettere eventuali certificati SSL/TLS
- L'indirizzo e-mail o l'URL da contattare quando un'autorità di certificazione emette un certificato per il dominio o il sottodominio.

Quando aggiungi un record CAA alle tue zona ospitata, devi specificare tre impostazioni separate da spazi:

```
flags tag "value"
```

Nota le seguenti informazioni sul formato per i record CAA:

- Il valore di `tag` può contenere solo i caratteri A - Z, a - z e 0-9.
- Racchiudi sempre `value` tra virgolette ("").
- Alcuni CAs consentono o richiedono valori aggiuntivi per. `value` Specifica i valori aggiuntivi come coppie nome-valore e separale con un punto e virgola (;), ad esempio:

  ```
  0 issue "ca.example.net; account=123456"
  ```
- Se una CA riceve una richiesta per un certificato per un sottodominio (ad esempio www.esempio.com) e non esistono record CAA per il sottodominio esistente, la CA invia una query DNS per un record CAA per il dominio padre (ad esempio esempio.com). Se un record

per il dominio padre esiste e la richiesta di certificato è valida, la CA emette il certificato per il sottodominio.

- Ti consigliamo di contattare la CA per determinare i valori da specificare per un record CAA.
- Non è possibile creare un record CAA e un record CNAME con lo stesso nome perché DNS non consente di utilizzare lo stesso nome per un record CNAME e per qualsiasi altro tipo di record.

Argomenti

- Autorizza una CA al rilascio di un certificato per un dominio o sottodominio
- Autorizza una CA al rilascio di un certificato jolly per un dominio o sottodominio
- Impedire a qualsiasi CA di emettere un certificato per un dominio o sottodominio
- Richiedere che una CA ti contatti se riceve una richiesta di certificato non valida
- Utilizzare un'altra impostazione supportata dalla CA
- Esempi

Autorizza una CA al rilascio di un certificato per un dominio o sottodominio

Per autorizzare una CA a rilasciare un certificato per un dominio o sottodominio, devi creare un record con lo stesso nome del dominio o del sottodominio e specificare le impostazioni seguenti:

- flag - `0`
- tag - `issue`
- value: il codice per la CA che autorizzi a emettere un certificato per il dominio o sottodominio

Ad esempio, supponiamo che desideri autorizzare ca.esempio.net a emettere un certificato per esempio.com. Devi creare un record CAA per esempio.com con le impostazioni seguenti:

```
0 issue "ca.example.net"
```

Per informazioni su come AWS Certificate Manager autorizzare l'emissione di un certificato, consulta Configurare un record CAA nella Guida per l'AWS Certificate Manager utente.

Autorizza una CA al rilascio di un certificato jolly per un dominio o sottodominio

Per autorizzare una CA a rilasciare un certificato jolly per un dominio o sottodominio, devi creare un record con lo stesso nome del dominio o del sottodominio e specificare le impostazioni seguenti. Un certificato jolly si applica al dominio o sottodominio e a tutti i suoi sottodomini.

- flag - `0`
- tag - `issuewild`
- value: il codice per la CA che autorizzi a emettere un certificato per un dominio o sottodominio e i relativi sottodomini

Ad esempio, supponiamo che desideri autorizzare ca.esempio.net a emettere un certificato jolly per esempio.com, che si applica a esempio.com e a tutti i suoi sottodomini. Devi creare un record CAA per esempio.com con le impostazioni seguenti:

```
0 issuewild "ca.example.net"
```

Se desideri autorizzare una CA a rilasciare un certificato jolly per un dominio o sottodominio, devi creare un record con lo stesso nome del dominio o del sottodominio e specificare le impostazioni seguenti. Un certificato jolly si applica al dominio o sottodominio e a tutti i suoi sottodomini.

Impedire a qualsiasi CA di emettere un certificato per un dominio o sottodominio

Per impedire a una CA di rilasciare un certificato jolly per un dominio o sottodominio, devi creare un record con lo stesso nome del dominio o del sottodominio e specificare le impostazioni seguenti:

- flag - `0`
- tag - `issue`
- Valore - `";"`

Ad esempio, supponiamo che non desideri che una CA emetta un certificato per esempio.com. Devi creare un record CAA per esempio.com con le impostazioni seguenti:

```
0 issue ";"
```

Se non desideri che una CA rilasci un certificato per esempio.com o i suoi sottodomini, devi creare un record CAA per esempio.com con le impostazioni seguenti:

```
0 issuewild ";"
```

> **Note**
>
> Se crei un record CAA per esempio.com e specifichi entrambi i seguenti valori, una CA che utilizza il valore ca.esempio.net può emettere il certificato per esempio.com:
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

Richiedere che una CA ti contatti se riceve una richiesta di certificato non valida

Se desideri che una CA che riceve una richiesta non valida per un certificato ti contattati, specifica le impostazioni seguenti:

- flag - `0`
- tag - `iodef`
- value: l'URL o l'indirizzo e-mail a cui desideri che la CA ti informi nel caso in cui riceve una richiesta non valida per un certificato. Utilizza il formato pertinente:

  `"mailto:`*`email-address`*`"`

  `"http://`*`URL`*`"`

  `"https://`*`URL`*`"`

Ad esempio, se desidera che una CA che riceve una richiesta non valida per un certificato invii e-mail ad admin@esempio.com, devi creare un record CAA con le impostazioni seguenti:

```
0 iodef "mailto:admin@example.com"
```

Utilizzare un'altra impostazione supportata dalla CA

Se la tua CA supporta una funzionalità che non è ancora definita nella RFC per i record CAA, specifica le impostazioni seguenti:

- flags: 128 (tale valore impedisce alla CA di rilasciare un certificato se non supporta la funzionalità specificata.)

- tag: il tag che autorizzi la CA a utilizzare
- value: il valore corrispondente al valore del tag

Ad esempio, supponiamo che la tua CA supporti l'invio di un messaggio di testo se la CA riceve una richiesta di certificato non valida. (Non siamo a conoscenza di nessuno CAs che supporti questa opzione). Le impostazioni per il record potrebbero essere le seguenti:

```
128 exampletag "15555551212"
```

Esempi

Esempio per la console Route 53

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Esempio per l'API Route 53

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

Tipo di record CNAME

Un record CNAME associa le query DNS relative al nome del record corrente, ad esempio acme.example.com, a un altro dominio (example.com o example.net) o sottodominio (acme.example.com o zenith.example.org).

> **Important**
>
> Il protocollo DNS non consente di creare un record CNAME per il nodo di primo livello di uno spazio di nomi DNS, noto anche come apex di zona. Ad esempio, se record il nome DNS esempio.com, l'apex di zona è esempio.com. Non puoi creare un record CNAME per esempio.com, ma puoi creare più record CNAME per www.esempio.com, nuovoprodotto.esempio.com e così via.
> Inoltre, se crei un record CNAME per un sottodominio, non puoi creare qualsiasi altro record per quel sottodominio. Ad esempio, se si crea un CNAME per www.example.com,

non è possibile creare altri record per i quali il valore del campo Name (Nome) è www.example.com.

Amazon Route 53 supporta anche i record di alias, che consentono di indirizzare le query a AWS risorse selezionate, come CloudFront distribuzioni e bucket Amazon S3. Gli alias sono simili in alcuni modi al tipo di record CNAME; tuttavia, puoi creare un alias per l'apex di zona. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Esempio per la console Route 53

```
hostname.example.com
```

Esempio per l'API Route 53

```
<Value>hostname.example.com</Value>
```

Tipo di record DS

Un record del firmatario della delega (DS) fa riferimento a una chiave di zona per una zona di sottodominio delegata. È possibile creare un record DS quando si stabilisce una catena di attendibilità quando si configura la firma DNSSEC. Per ulteriori informazioni sulla configurazione di DNSSEC in Route 53, consulta Configurazione della firma DNSSEC in Amazon Route 53.

I primi tre valori sono numeri decimali che rappresentano il tag della chiave, l'algoritmo e il tipo di digest. Il quarto valore è il digest della chiave di zona. Per ulteriori informazioni sul formato dei record DS, consulta RFC 4034.

Esempio per la console Route 53

```
123 4 5 1234567890abcdef1234567890absdef
```

Esempio per l'API Route 53

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

Tipo di record HTTPS

Un record di risorse HTTPS è una forma del record DNS Service Binding (SVCB) che fornisce informazioni di configurazione estese, consentendo a un client di connettersi in modo semplice

e sicuro a un servizio con un protocollo HTTP. Le informazioni di configurazione sono fornite in parametri che consentono la connessione in un'unica query DNS, anziché richiedere più query DNS.

Il formato per un record di risorse HTTPS è:

```
SvcPriority TargetName SvcParams(optional)
```

I seguenti parametri sono descritti nella RFC 9460, sezione 9.1.

SvcPriority

Un numero intero che rappresenta la priorità. La priorità 0 indica la modalità alias ed è generalmente destinata all'alias all'apice della zona. Questo valore è un numero intero 0-32767 per Route 53, di cui 1-32767 sono record in modalità servizio. Riduci la priorità, aumenta la preferenza.

TargetName

Il nome di dominio della destinazione dell'alias (per la modalità alias) o dell'endpoint alternativo (per). ServiceMode

SvcParams (facoltativo)

Un elenco separato da spazi bianchi, con ogni parametro costituito da una coppia Chiave=Valore o da una chiave autonoma. Se sono presenti più valori, vengono presentati come un elenco separato da virgole. I seguenti sono i definiti: SvcParams

- `1:alpn`— Protocollo di negoziazione del protocollo a livello di applicazione. IDs L'impostazione predefinita è HTTP/1.1, h2 è HTTP/2 su TLS e HTTP/3 (protocollo HTTP su h3 QUIC).
- `2:no-default-alpn`— L'impostazione predefinita non è supportata ed è necessario fornire un parametro. `alpn`
- `3:port`— l'endpoint alternativo o la porta da cui è possibile raggiungere il servizio.
- `4:ipv4hint`— suggerimenti sugli IPv4 indirizzi.
- `5:ech`— Client crittografato Hello.
- `6:ipv6hint`— suggerimenti IPv6 sugli indirizzi.
- `7:dohpath`— Modello DNS su HTTPS
- `8:ohttp`— Il servizio funziona con Oblivious HTTP target

Esempio di console Amazon Route 53 per la modalità alias

```
0 example.com
```

Esempio di console Amazon Route 53 per la modalità di servizio

```
16 example.com alpn="h2,h3" port=808
```

Esempio dell'API Amazon Route 53 per la modalità alias

```
<Value>0 example.com</Value>
```

Esempio dell'API Route 53 per la modalità di servizio

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Per ulteriori informazioni, vedere RFC 9460, Service Binding and Parameter Specification tramite DNS (SVCB e HTTPS Resource Records).

> **Note**
>
> Route 53 non supporta il formato arbitrario di presentazione a chiave sconosciuta `keyNNNNN`

Tipo di record MX

Un record MX specifica i nomi dei server di posta e, se si dispone di due o più server di posta, l'ordine di priorità. Ogni valore di un record MX include due valori: priorità e nome del dominio.

Priorità

Numero intero che rappresenta le priorità per un server di e-mail. Se specifichi solo un server, la priorità può essere un valore intero compreso tra 0 e 65535. Se specifichi più server, il valore specificato per la priorità indica per quali server e-mail desideri indirizzare le e-mail al primo, al secondo e così via. Il server con il valore più basso per la priorità ha la precedenza. Ad esempio, se disponi di due server e-mail e specifichi valori di 10 e 20 per la priorità, l'e-mail viene sempre inviata al server con una priorità di 10 a meno che non sia disponibile. Se specifichi valori di 10 e 10, l'e-mail viene instradata ai due server in modo praticamente uguale.

Nome dominio

Il nome di dominio del server e-mail. Specifica il nome (ad esempio mail.esempio.com) di un record A o AAAA. In RFC 2181, chiarimenti per la specifica DNS, la sezione 10.3 proibisce di specificare il nome di un record CNAME per il valore del nome di dominio. (Quando RFC cita "alias", significa un record CNAME, non un record alias di Route 53.)

Esempio per la console Amazon Route 53

```
10 mail.example.com
```

Esempio per l'API Route 53

```
<Value>10 mail.example.com</Value>
```

Tipo di record NAPTR

Un Name Authority Pointer (NAPTR) è un tipo di record utilizzato dalle applicazioni DDDS (Dynamic Delegation Discovery System) per convertire un valore in un altro valore o per sostituire un valore con un altro. Ad esempio, un uso comune è quello di convertire i numeri di telefono in SIP. URIs

L'elemento `Value` per un record NAPTR consiste in sei valori separati da spazio:

Order

Quando specifichi più di un record, la sequenza con cui desideri che l'applicazione DDDS valuti i record. Valori validi: 0-65535.

Preferenza

Quando specifichi due o più record con lo stesso Order (Ordine), le tue preferenze per la sequenza in cui questi record verranno valutati. Ad esempio, se due record hanno un Order (Ordine) di 1, l'applicazione DDDS prima valuta il record che ha la Preference (Preferenza) più bassa. Valori validi: 0-65535.

Flag

Impostazione specifica per le applicazioni DDDS. I valori attualmente definiti in RFC 3404 sono composti da lettere maiuscole e minuscole "A", "P", "S" e "U", e dalla stringa vuota, "". Includi Flags (Flag) tra virgolette.

Servizio

Impostazione specifica per le applicazioni DDDS. Includi Service (Servizio) tra virgolette.

Per ulteriori informazioni, consulta la pagina pertinente RFCs:

- Applicazione URI DDDS — https://tools.ietf.org/html/rfc3404 #section -4.4
- Applicazione DDDS S-NAPTR — /rfc3958 #section -6.5 https://tools.ietf.org/html
- Applicazione DDDS U-NAPTR — https://tools.ietf.org/html/rfc4848 #section -4.5

Regexp

Un'espressione regolare che l'applicazione DDDS impiega per convertire un valore di input in un valore di output. Ad esempio, un sistema telefonico IP potrebbe utilizzare un'espressione regolare per convertire un numero di telefono immesso da un utente in un URI SIP. Includi Regexp tra virgolette. Specifica un valore per Regexp o un valore per Replacement (Sostituzione), ma non entrambi.

L'espressione regolare può includere i seguenti caratteri ASCII stampabili:

- a-z
- 0-9
- - (trattino)
- (spazio)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (virgolette). Per includere virgolette in una stringa, è necessario anteporre un \ carattere: \".
- \ (barra rovesciata). Per includere una barra rovesciata in una stringa, è necessario anteporre un \ carattere: \\".

Specifica tutti gli altri valori, ad esempio i nomi di dominio internazionalizzati, in formato ottale.

Per la sintassi di Regexp, consulta la RFC 3402, sezione 3.2 Sintassi di espressione sostitutiva

Sostituzione

Il nome di dominio completo del prossimo nome di dominio per cui desideri che l'applicazione DDDS invii una query DNS. L'applicazione DDDS sostituisce il valore di input con il valore specificato per Replacement (Sostituzione). Specifica un valore per Regexp o un valore per Replacement (Sostituzione), ma non entrambi. Se specifichi un valore per Regexp, specifica un punto (.) per Replacement (Sostituzione).

Il nome di dominio può includere a-z, 0-9 e - (trattino).

Per ulteriori informazioni sulle applicazioni DDDS e sui record NAPTR, vedere quanto segue: RFCs

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Esempio per la console Amazon Route 53

```
100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Esempio per l'API Route 53

```
<ResourceRecord>
   <Value>100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .</Value>
   <Value>100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .</
Value>
   <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

Tipo di record NS

Un record NS identifica i server di nomi per la zona ospitata. Tieni presente quanto segue:

- Un record NS viene utilizzato il più delle volte per controllare la modalità di instradamento del traffico Internet per un dominio. Se si desidera utilizzare i record in una zona ospitata per instradare il traffico per un dominio, è possibile aggiornare le impostazioni di registrazione del dominio per utilizzare i quattro server dei nomi nel record NS predefinito (si tratta del record NS che ha lo stesso nome della zona ospitata).
- È possibile creare una zona ospitata separata per un sottodominio (acme.example.com) e utilizzarla per instradare il traffico Internet per il sottodominio e i relativi sottodomini (subdomain.acme.example.com). È possibile impostare questa configurazione, nota come “delegazione della responsabilità di un sottodominio a una zona ospitata”, creando un altro record

NS nella zona ospitata per il dominio radice (example.com). Per ulteriori informazioni, consulta Routing del traffico per sottodomini.

- È inoltre possibile utilizzare i record NS per configurare i server dei nomi white label. Per ulteriori informazioni, consulta Configurazione dei server di nomi white label.

Per ulteriori informazioni sui record NS, consulta Record NS e SOA creati da Amazon Route 53 per una zona ospitata pubblica.

Esempio per la console Amazon Route 53

```
ns-1.example.com
```

Esempio per l'API Route 53

```
<Value>ns-1.example.com</Value>
```

Tipo di record PTR

Un record PTR associa un indirizzo IP al nome di dominio corrispondente.

Esempio per la console Amazon Route 53

```
hostname.example.com
```

Esempio per l'API Route 53

```
<Value>hostname.example.com</Value>
```

Tipo di record SOA

Un record di origine di autorità (SOA) fornisce informazioni su un dominio e la zona ospitata Amazon Route 53 corrispondente. Per ulteriori informazioni sui campi in un record SOA, consulta Record NS e SOA creati da Amazon Route 53 per una zona ospitata pubblica.

Esempio per la console Route 53

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Esempio per l'API Route 53

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

Tipo di record SPF

I record SPF erano precedentemente usati per verificare l'identità del mittente di messaggi e-mail. Tuttavia, non è più consigliabile creare record per i quali il tipo di record è SPF. La RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, versione 1, è stata aggiornata per dire: «... [La] sua esistenza e il meccanismo definiti in [RFC4408] hanno portato ad alcuni problemi di interoperabilità. Di conseguenza, il suo utilizzo non è più appropriato per SPF versione 1; le implementazioni non devono utilizzarlo." In RFC 7208, consulta la sezione 14.1, Tipo record DNS SPF.

Invece di un record SPF, è consigliabile creare un record TXT che contiene il valore applicabile. Per ulteriori informazioni sui valori validi, consulta l'articolo Wikipedia Sender Policy Framework.

Esempio per la console Amazon Route 53

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Esempio per l'API Route 53

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Tipo di record SRV

Un record `Value` SRV consiste in quattro valori separati da spazio. I primi tre valori sono numeri decimali con priorità, peso e porta. Il quarto valore è un nome di dominio. I record SRV vengono utilizzati per accedere a servizi, ad esempio un servizio per e-mail o comunicazioni. Per informazioni sul formato dei record SRV, consulta la documentazione relativa al servizio a cui desideri connetterti.

Esempio per la console Amazon Route 53

```
10 5 80 hostname.example.com
```

Esempio per l'API Route 53

```
<Value>10 5 80 hostname.example.com</Value>
```

Tipo di record SSHFP

Un record di impronte digitali Secure Shell (SSHFP) identifica le chiavi SSH associate al nome di dominio. I record SSHFP devono essere protetti con DNSSEC per stabilire una catena di fiducia. Per ulteriori informazioni su DNSSEC, vedere Configurazione della firma DNSSEC in Amazon Route 53

Il formato per un record di risorse SSHFP è:

```
[Key Algorithm] [Hash Type] Fingerprint
```

I seguenti parametri sono definiti nella RFC 4255.

Algoritmo chiave

Tipo di algoritmo:

- `0`— Riservato e non utilizzato.
- `1: RSA`— L'algoritmo Rivest-Shamir-Adleman è uno dei primi sistemi crittografici a chiave pubblica ed è ancora utilizzato per la trasmissione sicura dei dati.
- `2: DSA`— L'algoritmo di firma digitale è uno standard federale di elaborazione delle informazioni per le firme digitali. Il DSA si basa sull'esponenziazione modulare e sui modelli matematici a logaritmi discreti.
- `3: ECDSA`— Elliptic Curve Digital Signature Algorithm è una variante del DSA che utilizza la crittografia a curva ellittica.
- `4: Ed25519`— L'algoritmo Ed25519 è lo schema di firma EdDSA che utilizza SHA-512 (SHA-2) e Curve25519.
- `6: Ed448`— Ed448 è lo schema di firma EdDSA che utilizza e Curve448. SHAKE256

Tipo di hash

Algoritmo utilizzato per creare l'hash della chiave pubblica:

- `0`—Riservato e non utilizzato.
- `1: SHA-1`
- `2: SHA-256`

Impronta digitale

Rappresentazione esadecimale dell'hash.

Esempio per la console Amazon Route 53

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Esempio per l'API Route 53

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

Per ulteriori informazioni, vedere RFC 4255: Utilizzo del DNS per pubblicare in modo sicuro le impronte digitali delle chiavi Secure Shell (SSH).

Tipo di record SVCB

Si utilizza un record SVCB per fornire informazioni di configurazione per l'accesso agli endpoint del servizio. SVCB è un record DNS generico e può essere utilizzato per negoziare i parametri per una varietà di protocolli applicativi.

Il formato per un record di risorse SVCB è:

`SvcPriority TargetName SvcParams(optional)`

I seguenti parametri sono descritti nella RFC 9460, sezione 2.3.

SvcPriority

Un numero intero che rappresenta la priorità. La priorità 0 indica la modalità alias ed è generalmente destinata all'alias all'apice della zona. Abbassa la priorità, aumenta la preferenza.

TargetName

Il nome di dominio della destinazione dell'alias (per la modalità alias) o dell'endpoint alternativo (per). ServiceMode

SvcParams (facoltativo)

Un elenco separato da spazi bianchi, con ogni parametro costituito da una coppia Chiave=Valore o da una chiave autonoma. Se sono presenti più valori, vengono presentati come un elenco separato da virgole. Questo valore è un numero intero 0-32767 per la Route 53, di cui 1-32767 sono record in modalità servizio. I seguenti sono i definiti: SvcParams

- `1:alpn`— Protocollo di negoziazione del protocollo a livello di applicazione. IDs L'impostazione predefinita è HTTP/1.1, h2 è HTTP/2 su TLS e HTTP/3 (protocollo HTTP su h3 QUIC).
- `2:no-default-alpn`— L'impostazione predefinita non è supportata ed è necessario fornire un parametro. `alpn`

- `3:port`— la porta per l'endpoint alternativo in cui è possibile raggiungere il servizio.
- `4:ipv4hint`— suggerimenti sugli IPv4 indirizzi.
- `5:ech`— Client crittografato Hello.
- `6:ipv6hint`— suggerimenti IPv6 sugli indirizzi.
- `7:dohpath`— Modello DNS su HTTPS
- `8:ohttp`— Il servizio gestisce un target HTTP Oblivious

Esempio di console Amazon Route 53 per la modalità alias

```
0 example.com
```

Esempio di console Amazon Route 53 per la modalità di servizio

```
16 example.com alpn="h2,h3" port=808
```

Esempio dell'API Amazon Route 53 per la modalità alias

```
<Value>0 example.com</Value>
```

Esempio dell'API Route 53 per la modalità di servizio

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

Per ulteriori informazioni, vedere RFC 9460, Service Binding and Parameter Specification tramite DNS (SVCB e HTTPS Resource Records).

> **Note**
>
> Route 53 non supporta il formato arbitrario di presentazione a chiave sconosciuta `keyNNNNN`

Tipo di record TLSA

Si utilizza un record TLSA per utilizzare l'autenticazione delle entità denominate (DANE) basata su DNS. Un record TLSA associa una certificate/public key with a Transport Layer Security (TLS)

endpoint, and clients can validate the certificate/public chiave utilizzando un record TLSA firmato con DNSSEC.

I record TLSA possono essere considerati attendibili solo se DNSSEC è abilitato sul dominio. Per ulteriori informazioni su DNSSEC, vedere Configurazione della firma DNSSEC in Amazon Route 53

Il formato per un record di risorse TLSA è:

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

I seguenti parametri sono specificati nella RFC 6698, sezione 3.

Utilizzo del certificato

Speciifica l'associazione fornita che verrà utilizzata per abbinare il certificato presentato nell'handshake TLS:

- 0: vincolo CA: il certificato o la chiave pubblica devono essere trovati in uno qualsiasi dei percorsi di certificazione PKIX (Public Key Infrastructure) per il certificato dell'entità finale fornito dal server in TLS. Questo vincolo limita i dati che CAs possono essere utilizzati per emettere certificati per un servizio specifico.
- 1: Vincolo del certificato di entità finale: specifica un certificato di entità finale (o la chiave pubblica) che deve corrispondere al certificato dell'entità finale fornito dal server in TLS. Questa certificazione limita il certificato dell'entità finale che può essere utilizzato da un servizio specifico su un host.
- 2: Un'asserzione di trust Anchor: specifica un certificato (o la chiave pubblica) che deve essere utilizzato come «trust anchor» durante la convalida del certificato di entità finale fornito dal server in TLS. Consente a un amministratore di dominio di specificare un trust anchor.
- 3: Certificazione rilasciata dal dominio: specifica un certificato (o la chiave pubblica) che deve corrispondere al certificato dell'entità finale fornito dal server in TLS. Questa certificazione consente a un amministratore di dominio di emettere certificati per un dominio senza coinvolgere una CA di terze parti. Non è necessario che questo certificato superi la convalida PKIX.

Selector

Speciifica quale parte del certificato presentato dal server nell'handshake corrisponde al valore dell'associazione:

- 0: è necessario abbinare l'intero certificato.
- 1: La chiave pubblica del soggetto, o la struttura binaria con codifica DER, deve corrispondere.

Tipo corrispondente

Speciifica la presentazione (come determinata dal campo Selector) della corrispondenza del certificato:

- 0: Corrispondenza esatta del contenuto.
- 1: hash SHA-256.
- 2: hash SHA-512.

Dati di associazione dei certificati

I dati da abbinare in base alle impostazioni degli altri campi.

Esempio per la console Amazon Route 53

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Esempio per l'API Route 53

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

Per ulteriori informazioni, vedere RFC 6698, The DNS-based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.

Tipo di record TXT

Un record TXT contiene una o più stringhe racchiuse tra virgolette ('"'). Quando utilizzi la policy di routing semplice, includi tutti i valori per un dominio (esempio.com) o sottodominio (www.esempio.com) nello stesso record TXT.

Argomenti

- Inserimento dei valori del record TXT
- Caratteri speciali in un valore di record TXT
- Maiuscole e minuscole in un valore di record TXT
- Esempi

Inserimento dei valori del record TXT

Una singola stringa può includere fino a 255 caratteri, tra cui i seguenti:

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

Se è necessario immettere un valore più lungo di 255 caratteri, suddividere il valore in stringhe di 255 caratteri o numero inferiore e racchiudere ogni stringa tra virgolette doppie ("). Nella console, elencare tutte le stringhe sulla stessa riga:

```
"String 1" "String 2" "String 3"
```

Per l'API, includere tutte le stringhe nello stesso elemento `Value`:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

La lunghezza massima di un valore in un record TXT è di 4.000 caratteri.

Per inserire più di un valore TXT, inserisci un valore per riga.

Caratteri speciali in un valore di record TXT

Se il record TXT contiene uno dei seguenti caratteri, è necessario specificare i caratteri utilizzando i codici di escape nel formato: \ *three-digit octal code*

- Caratteri da 000 a 040 ottali (da 0 a 32 decimali, da 0x00 a 0x20 esadecimali)
- Caratteri da 177 a 377 ottali (da 127 a 255 decimali, da 0x7F a 0xFF esadecimali)

Ad esempio, se il valore del tuo record TXT è `"exämple.com"`, devi specificare `"ex\344mple.com"`.

Per una mappatura tra caratteri ASCII e codici ottali, esegui una ricerca su Internet per «codici ottali ASCII». Un utile riferimento è la tabella estesa dei codici ASCII.

Per includere le virgolette (") in una stringa, inserisci una barra rovesciata (\) prima della virgoletta: \".

Maiuscole e minuscole in un valore di record TXT

Maiuscole e minuscole vengono mantenute, perciò `"Ab"` e `"aB"` sono valori diversi.

Esempi

Esempio per la console Amazon Route 53

Immetti ogni valore su una riga distinta:

```
"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"
```

Esempio per l'API Route 53

Immetti ogni valore in un elemento `Value` separato:

```
<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>
```

Creazione di record utilizzando la console Amazon Route 53

La procedura seguente spiega come creare record utilizzando la console Amazon Route 53. Per informazioni su come creare record utilizzando l'API Route 53, consulta ChangeResourceRecordSetsAmazon Route 53 API Reference.

> **Note**
>
> Per creare record per configurazioni di routing complesse, puoi usare il l'editor visivo del flusso di traffico e salvare la configurazione come una policy di traffico. Puoi quindi associare la policy di traffico a uno o più nomi di dominio (ad esempio esempio.com) o nomi di sottodominio (ad esempio www.esempio.com), nella stessa zona ospitata o in più zone ospitate. Inoltre, puoi eseguire il roll back degli aggiornamenti se la nuova configurazione non offre le prestazioni previste. Per ulteriori informazioni, consulta Utilizzo di Traffic Flow per instradare il traffico DNS.

Come creare un record mediante la console Route 53

1. Se non stai creando un record alias, passa al punto 2.

   Vai anche al passaggio 2 se stai creando un record di alias che indirizza il traffico DNS verso una AWS risorsa diversa da un sistema di bilanciamento del carico Elastic Load Balancing o un altro record Route 53.

   Quando crei un record alias che instrada il traffico a un sistema di bilanciamento del carico Elastic Load Balancing, se hai creato la zona ospitata e il sistema di bilanciamento del carico utilizzando account diversi, esegui la procedura Come ottenere il nome DNS per un sistema di bilanciamento del carico Elastic Load Balancing per ottenere il nome DNS per il sistema di bilanciamento del carico.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Se si dispone già di una zona ospitata per il dominio, passare alla fase 5. In caso contrario, eseguire la procedura applicabile per creare una zona ospitata:

   - Per indirizzare il traffico Internet verso le tue risorse, come i bucket Amazon S3 o le EC2 istanze Amazon, consulta. Creazione di una zona ospitata pubblica
   - Per instradare il traffico nel VPC, consulta Creazione di una zona ospitata privata.
5. Nella pagina Zone ospitate, scegli il nome della zona ospitata in cui desideri creare i record.
6. Scegli Crea record.
7. Scegli e definisci la policy di routing e i valori applicabili. Per ulteriori informazioni, consulta l'argomento per il tipo di record che desideri creare:

   - Valori comuni per tutte le policy di routing
   - Valori comuni per i record alias per tutte le policy di routing
   - Valori specifici per record semplici
   - Valori specifici per record alias semplici
   - Valori specifici per record di failover
   - Valori specifici per i record alias di failover
   - Valori specifici per record di geolocalizzazione
   - Valori specifici per record degli alias di geolocalizzazione

- Valori specifici per i record di geoprossimità
- Valori specifici per i record di alias di geoprossimità
- Valori specifici per i record di latenza
- Valori specifici per i record alias di latenza
- Valori specifici per i record basati su IP
- Valori specifici per i record alias basati su IP
- Valori specifici per record di risposta multivalore
- Valori specifici per record ponderati
- Valori specifici per i record alias ponderati

8. Scegli Crea record.

> **Note**
>
> I tuoi nuovi record richiedono tempo per propagarsi ai server DNS di Route 53. Attualmente, l'unico modo per verificare che le modifiche si siano propagate consiste nell'utilizzare l'azione API. GetChange In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

9. Se stai creando più record, ripeti le fasi da 7 a 8.

Come ottenere il nome DNS per un sistema di bilanciamento del carico Elastic Load Balancing

1. Accedi AWS Management Console utilizzando l' AWS account utilizzato per creare il Classic, Application o Network Load Balancer per cui desideri creare un record di alias.
2. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
3. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
4. Nell'elenco dei sistemi di load balancer, seleziona il load balancer per cui desideri creare un record alias.
5. Nella scheda Description (Descrizione), ottieni il valore di DNS name (Nome DNS).
6. Se desideri creare record alias per altri sistemi di bilanciamento del carico Elastic Load Balancing, ripeti i passaggi 4 e 5.
7. Esci da AWS Management Console.
8. Accedi AWS Management Console nuovamente utilizzando l' AWS account che hai usato per creare la zona ospitata da Route 53.

9. Torna al passo 3 della procedura Creazione di record utilizzando la console Amazon Route 53.

Autorizzazioni del set di record di risorse

Le autorizzazioni relative ai set di record di risorse utilizzano le condizioni delle policy di gestione delle identità e degli accessi (IAM) per consentire di impostare autorizzazioni granulari per le azioni sulla console Route 53 o per l'utilizzo dell'API. ChangeResourceRecordSets

Un set di record di risorse è definito come più record di risorse con lo stesso nome e tipo (e classe, ma per la maggior parte degli scopi la classe è sempre IN o Internet) che contengono però dati diversi. Ad esempio, se scegli l'instradamento basato sulla geolocalizzazione, puoi avere più record A o AAAA che puntano a endpoint diversi per lo stesso dominio. Tutti questi record A o AAAA si combinano per formare un set di record di risorse. Per ulteriori informazioni sulla terminologia DNS, consulta RFC 7719.

Con le condizioni delle policy IAM,`route53:ChangeResourceRecordSetsNormalizedRecordNames`, and `route53:ChangeResourceRecordSetsRecordTypesroute53:ChangeResourceRecordSetsActio` puoi concedere diritti amministrativi granulari ad altri AWS utenti in qualsiasi altro account. AWS Ciò consente di concedere a qualcuno le autorizzazioni per:

- Un singolo set di record di risorse.
- Tutti i set di record di risorse di un tipo di record DNS specifico.
- Set di record di risorse in cui i nomi contengono una stringa specifica.
- Esegui alcune o tutte le `CREATE | UPSERT | DELETE` azioni quando usi l'ChangeResourceRecordSetsAPI o la console Route 53.

Puoi anche creare autorizzazioni di accesso che combinano qualsiasi condizione delle policy di Route 53. Ad esempio, puoi concedere a qualcuno le autorizzazioni per modificare i dati del record A per marketing-example.com, ma non consentire all'utente di eliminare i record.

Per ulteriori informazioni sulle autorizzazioni relative ai set di record di risorse ed esempi su come utilizzarle, consultaUtilizzo di condizioni di policy IAM per il controllo granulare degli accessi.

Per informazioni su come autenticare AWS gli utenti, consulta Autenticazione con identità e per imparare a controllare l'accesso alle risorse di Route 53, consulta. Controllo accessi

Di seguito sono descritti i valori che devi specificare durante la creazione o la modifica di record di Amazon Route 53.

Quando crei record utilizzando la console Amazon Route 53, i valori specificati dipendono dalla politica di routing che desideri utilizzare e dal fatto che tu stia creando record di alias, che indirizzano il traffico verso AWS le risorse.

Record di alias che indirizzano il traffico verso determinate AWS risorse per le quali si specifica la risorsa di destinazione (ad esempio, Elastic Load Balancing CloudFront , distribuzione, bucket Amazon S3). Facoltativamente, puoi anche associare i controlli di integrità e configurare la valutazione dello stato dell'obiettivo. I seguenti argomenti forniscono informazioni dettagliate sui valori richiesti per ogni politica di routing e tipo di record, aiutandoti a configurare i record della Route 53 in modo efficace.

Argomenti

Valori comuni per tutte le policy di routing

Questi sono i valori comuni che puoi specificare durante la creazione o la modifica di record di Amazon Route 53. Questi valori sono utilizzati da tutte le policy di routing.

Argomenti

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Registri CNAME

Se stai creando un record che ha lo stesso valore di CNAME per Tipo di record, il nome del record non può essere uguale al nome della zona ospitata.

Caratteri speciali

Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

Caratteri jolly

Puoi utilizzare un asterisco (*) all'interno del nome. Il DNS considera il carattere * sia come un carattere jolly che come il carattere * (ASCII 42), a seconda della posizione nel nome. Per ulteriori informazioni, consulta Utilizza un asterisco (*) nei nomi di zone ospitate e registri.

> **Important**
>
> Non puoi utilizzare il carattere jolly * per set di record della risorsa che sono di tipo NS.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

A — IPv4 indirizzo

Un indirizzo IP in IPv4 formato, ad esempio 192.0.2.235.

AAAA: IPv6 indirizzo

Un indirizzo IP in IPv6 formato, ad esempio, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334.

CAA - Autorizzazione della certification authority

Tre valori separati da spazi che determinano le autorità di certificazione a cui è consentito emettere certificati o certificati con caratteri jolly per il dominio o il sottodominio specificato da Nome record. Puoi utilizzare i record CAA per specificare quanto segue:

- Quali autorità CAs di certificazione () possono emettere eventuali certificati SSL/TLS
- L'indirizzo e-mail o l'URL da contattare quando un'autorità di certificazione emette un certificato per il dominio o il sottodominio.

CNAME - Nome canonico

Il nome di dominio completo (come www.esempio.com) che Route 53 deve restituire in risposta alle query DNS per questo record. Un punto finale è facoltativo; Route 53 presuppone che il nome dominio sia completo. Ciò significa che Route 53 considera identici www.esempio.com (senza un punto finale) e www.esempio.com. (con un punto finale).

MX - Scambio di posta

Una priorità e un nome di dominio che specifica un server di posta, ad esempio 10 mailserver.example.com. Il punto finale viene trattato come facoltativo.

NAPTR - Puntatore dell'autorità dei nomi

Sei impostazioni separate da spazi utilizzate dalle applicazioni DDDS (Dynamic Delegation Discovery System) per convertire un valore in un altro valore o per sostituire un valore con un altro. Per ulteriori informazioni, consulta Tipo di record NAPTR.

PTR - Puntatore

Il nome dominio che desideri sia restituito da Route 53.

NS - Server di nomi

Il nome di dominio di un server dei nomi, ad esempio ns1.example.com.

> **Note**
>
> È possibile specificare un registro NS con solo una policy di routing semplice.

SPF - Sender Policy Framework

Un record SPF racchiuso tra virgolette, ad esempio "v=spf1 ip4:192.168.0.1/16-all". L'utilizzo di record SPF non è consigliato. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

SRV - Localizzatore di servizi

Un record SRV. I record SRV vengono utilizzati per accedere a servizi, ad esempio un servizio per e-mail o comunicazioni. Per informazioni sul formato dei record SRV, consulta la documentazione relativa al servizio a cui desideri connetterti. Il punto finale viene trattato come facoltativo.

Il formato di un record SRV è:

[priority] [weight] [port] [server host name]

Ad esempio:

1 10 5269 xmpp-server.example.com.

TXT - Testo

Un record di testo. Racchiudi il testo tra virgolette, ad esempio "Esempio di immissione di testo".

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i

valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valori comuni per i record alias per tutte le policy di routing

Questi sono i valori alias comuni che devi specificare durante la creazione o la modifica di record di Amazon Route 53. Questi valori sono utilizzati da tutte le policy di routing.

Argomenti

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Registri CNAME

Se stai creando un record che ha lo stesso valore di CNAME per Type (Tipo), il nome del record non può essere uguale al nome della zona ospitata.

Alias per CloudFront distribuzioni e bucket Amazon S3

Il valore specificato dipende in parte dalla AWS risorsa verso cui stai indirizzando il traffico:

- CloudFront distribuzione: la distribuzione deve includere un nome di dominio alternativo che corrisponda al nome del record. Ad esempio, se il nome del record è acme.example.com, la distribuzione CloudFront deve includere acme.example.com come uno dei nomi di dominio alternativi. Per ulteriori informazioni, consulta Using alternate domain names (CNAMEs) nella Amazon CloudFront Developer Guide.
- Bucket Amazon S3: il nome del record deve corrispondere al nome del bucket Amazon S3. Ad esempio, se il nome del bucket è acme.example.com, anche il nome del record deve essere acme.example.com.

Inoltre, devi configurare il bucket per l'hosting di siti Web. Per ulteriori informazioni, consulta Configurazione di un bucket per l'hosting di un sito Web nella Guida per utenti di Amazon Simple Storage Service.

Caratteri speciali

Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

Caratteri jolly

Puoi utilizzare un asterisco (*) all'interno del nome. Il DNS considera il carattere * sia come un carattere jolly che come il carattere * (ASCII 42), a seconda della posizione nel nome. Per ulteriori informazioni, consulta Utilizza un asterisco (*) nei nomi di zone ospitate e registri.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consultaInstradamento del traffico Internet verso le tue risorse AWS.

Important

Se hai utilizzato lo stesso AWS account per creare la tua zona ospitata e la risorsa verso cui stai indirizzando il traffico e se la risorsa non compare nell'elenco degli endpoint, controlla quanto segue:

- Conferma di aver scelto un valore supportato per Tipo di record. I valori supportati sono specifici della risorsa a cui si sta instradando il traffico. Ad esempio, per indirizzare il traffico verso un bucket S3, devi scegliere A — IPv4 indirizzo per Tipo di record.
- Confermare che l'account disponga delle autorizzazioni IAM necessarie per elencare le risorse applicabili. Ad esempio, affinché le distribuzioni CloudFront vengano visualizzate nell'elenco Endpoint, l'account deve disporre dell'autorizzazione per l’esecuzione della seguente azione: `cloudfront:ListDistributions`.

  Per un esempio di policy IAM, consultare Autorizzazioni necessarie per utilizzare la console Amazon Route 53.

Se hai utilizzato AWS account diversi per creare la zona ospitata e la risorsa, l'elenco degli endpoint non mostra la tua risorsa. Consulta la seguente documentazioni relativa al tipo di risorsa per stabilire il valore da immettere in Endpoint.

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Per API Gateway personalizzato, regionale APIs e ottimizzato per i dispositivi perimetrali APIs, effettuate una delle seguenti operazioni:

- Se hai usato lo stesso account per creare la zona ospitata Route 53 e l'API: scegli Endpoint, e seleziona quindi un'API dall'elenco. Se ne hai molti APIs, puoi inserire i primi caratteri dell'endpoint API per filtrare l'elenco.

  > **Note**
  >
  > Il nome del record che stai creando deve corrispondere a un nome di dominio personalizzato per la tua API, ad esempio api.example.com.

- Se hai utilizzato account diversi per creare la tua zona ospitata Route 53 e la tua API: inserisci l'endpoint dell'API per l'API, ad esempio api.example.com.

  Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare un'API, l'API non verrà visualizzata nell'elenco degli endpoint in API Gateway APIs.

  Se hai utilizzato un account per creare la zona ospitata corrente e uno o più account diversi per creare tutti i tuoi APIs, l'elenco degli endpoint mostra Nessun target disponibile in API Gateway APIs. Per ulteriori informazioni, consulta Routing del traffico a un'API di Amazon API Gateway usando il proprio nome di dominio.

CloudFront distribuzioni

Per CloudFront le distribuzioni, effettuate una delle seguenti operazioni:

- Se hai utilizzato lo stesso account per creare la zona ospitata su Route 53 e la tua CloudFront distribuzione, scegli Endpoint e scegli una distribuzione dall'elenco. Se disponi di molte distribuzioni, puoi inserire i primi caratteri del nome del dominio per la distribuzione per filtrare l'elenco.

  Se la distribuzione non appare nell'elenco, tieni presente quanto segue:

- Il nome di questo record deve corrispondere a un nome di dominio alternativo nella distribuzione.
- Se hai appena aggiunto un nome di dominio alternativo alla tua distribuzione, potrebbero essere necessari 15 minuti prima che le modifiche si propaghino a tutte le CloudFront edge location. Fino a quando le modifiche non si sono propagate, Route 53 non può conoscere il nuovo nome di dominio alternativo.

- Se hai utilizzato account diversi per creare la zona ospitata su Route 53 e la tua distribuzione, inserisci il nome di CloudFront dominio per la distribuzione, ad esempio d111111abcdef8.cloudfront.net.

  Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare una distribuzione, la distribuzione non verrà visualizzata nell'elenco degli endpoint.

  Se hai utilizzato un account per creare la zona ospitata corrente e uno o più account diversi per creare tutte le distribuzioni, l'elenco degli endpoint mostra Nessun obiettivo disponibile nelle distribuzioni. CloudFront

> **Important**
>
> Non indirizzate le query a una CloudFront distribuzione che non si è propagata a tutte le edge location, altrimenti gli utenti non saranno in grado di accedere al contenuto applicabile.

La tua CloudFront distribuzione deve includere un nome di dominio alternativo che corrisponda al nome del record. Ad esempio, se il nome del record è acme.example.com, la CloudFront distribuzione deve includere acme.example.com come uno dei nomi di dominio alternativi. Per ulteriori informazioni, consulta Using alternate domain names (CNAMEs) nella Amazon CloudFront Developer Guide.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A — IPv4 indirizzo per il tipo di record e uno con un valore di AAAA — IPv6 indirizzo. Per ulteriori informazioni, consulta Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio.

Servizio App Runner

Per il servizio App Runner, esegui una delle seguenti operazioni:

- Se hai utilizzato lo stesso account per creare la zona ospitata su Route 53 e il servizio App Runner Regione AWS, scegli il, quindi scegli il nome di dominio dell'ambiente verso cui indirizzare il traffico dall'elenco.
- Se hai utilizzato account diversi per creare la tua zona ospitata su Route 53 e il tuo App Runner, inserisci il nome di dominio personalizzato. Per ulteriori informazioni, consulta Gestione di nomi di dominio personalizzati per App Runner.

  Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare un App Runner, l'App Runner non verrà visualizzato nell'elenco degli endpoint.

Per ulteriori informazioni, consulta Configurazione di Amazon Route 53 per instradare il traffico a un servizio App Runner.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se il nome di dominio per l'ambiente Elastic Beanstalk comprende la regione in cui hai distribuito l'ambiente, puoi creare un record alias che instrada il traffico verso l'ambiente. Ad esempio, il nome di dominio `my-environment.us-west-2.elasticbeanstalk.com` è un nome di dominio regionalizzato.

> **Important**
>
> Per gli ambienti creati prima dell'inizio del 2016, il nome di dominio non include la regione. Per instradare il traffico verso questi ambienti, è necessario creare un record CNAME invece di un record alias. Non puoi creare un record CNAME per il nome di dominio root. Ad esempio, se il tuo nome di dominio è esempio.com, è possibile creare un record che consente di instradare il traffico per acme.esempio.com al tuo ambiente Elastic Beanstalk, ma non potrai creare un record che consente di instradare il traffico per esempio.com al tuo ambiente Elastic Beanstalk.

Per gli ambienti Elastic Beanstalk che hanno sottodomini regionalizzati, procedi in uno dei modi seguenti:

- Se hai usato lo stesso account per creare la zona ospitata Route 53 e l'ambiente Elastic Beanstalk: scegli Endpoint e seleziona quindi un ambiente dall'elenco. Se disponi di molti ambienti, puoi inserire i primi caratteri dell'attributo CNAME affinché l'ambiente filtri l'elenco.
- Se hai usato diversi account per creare la tua zona ospitata Route 53 e l'ambiente Elastic Beanstalk_ specifica l'attributo CNAME per l'ambiente Elastic Beanstalk.

Per ulteriori informazioni, consulta Instradamento del traffico verso un ambiente AWS Elastic Beanstalk.

load balancer ELB

Per i sistemi di bilanciamento del carico ELB, procedere in uno dei seguenti modi:

- Se hai usato lo stesso account per creare la zona ospitata Route 53 e il load balancer: scegli Endpoint e seleziona un load balancer dall'elenco. Se disponi di molti sistemi di bilanciamento del carico, puoi inserire i primi caratteri del nome DNS per filtrare l'elenco.
- Se hai usato diversi account per creare la tua zona ospitata Route 53 e il load balancer: inserisci il valore ottenuto nella procedura Come ottenere il nome DNS per un sistema di bilanciamento del carico Elastic Load Balancing.

  Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare un sistema di bilanciamento del carico, il sistema di bilanciamento del carico non verrà visualizzato nell'elenco degli endpoint.

  Se hai utilizzato un account per creare la zona ospitata corrente e uno o più account diversi per creare tutti i bilanciatori del carico, nell'elenco Endpoints viene visualizzato Nessuna destinazione disponibile in Elastic Load Balancer.

La consolle aggiunge dualstack. per Application Load Balancer e Classic Load Balancer da un diverso account. Quando un client, ad esempio un browser Web, richiede l'indirizzo IP per il nome di dominio (esempio.com) o il nome di sottodominio (www.esempio.com), il client può richiedere un IPv4 indirizzo (un record A), un IPv6 indirizzo (un record AAAA) o entrambi IPv4 gli IPv6 indirizzi (in richieste separate). La designazione dualstack. consente a Route 53 di rispondere con l'indirizzo IP appropriato per il load balancer in base al formato dell'indirizzo IP richiesto dal client.

Per ulteriori informazioni, consulta Routing del traffico a un load balancer ELB.

AWS Acceleratori Global Accelerator

Per gli acceleratori AWS Global Accelerator, inserisci il nome DNS dell'acceleratore. Puoi inserire il nome DNS di un acceleratore creato utilizzando l' AWS account corrente o utilizzando un account diverso. AWS

Bucket Amazon S3

Per i bucket Amazon S3 che sono configurati come endpoint del sito Web, procedi in uno dei modi seguenti:

- Se hai usato lo stesso account per creare la zona ospitata Route 53 e il bucket Amazon S3: scegli Endpoint e seleziona quindi un bucket dall'elenco. Se disponi di molti bucket, puoi inserire i primi caratteri del nome DNS per filtrare l'elenco.

  Il valore di Endpoint diventa l'endpoint del sito Web Amazon S3 per il bucket.

- Se hai usato diversi account per creare la tua zona ospitata Route 53 e il bucket Amazon S3 - inserisci il nome della regione nella quale hai creato il bucket S3. Utilizza il valore che appare nella colonna Endpoint sito web nella tabella Endpoint del sito web Amazon S3 in Riferimenti generali di Amazon Web Services.

  Se hai utilizzato AWS account diversi dall'account corrente per creare i tuoi bucket Amazon S3, il bucket non verrà visualizzato nell'elenco degli endpoint.

Devi configurare il bucket per l'hosting di siti Web. Per ulteriori informazioni, consulta Configurazione di un bucket per l'hosting di un sito Web nella Guida per utenti di Amazon Simple Storage Service.

Il nome del record deve corrispondere al nome del bucket Amazon S3. Ad esempio, se il nome del bucket Amazon S3 è acme.esempio.com, anche il nome del record deve essere acme.esempio.com.

In un gruppo di alias ponderati, alias di latenza, alias di failover o alias di geolocalizzazione, puoi creare un solo record che instrada le query a un bucket Amazon S3 perché il nome del record deve corrispondere al nome del bucket e nomi dei bucket devono essere globalmente univoci.

OpenSearch Servizio Amazon

Per OpenSearch Service, esegui una delle seguenti operazioni:

- OpenSearch Dominio personalizzato del servizio: il nome del record deve corrispondere al dominio personalizzato. Ad esempio, se il nome del dominio personalizzato è test.example.com, anche il nome di questo record deve essere test.example.com.
- Se hai utilizzato lo stesso account per creare la zona ospitata su Route 53 e il dominio di OpenSearch servizio, scegli il, quindi scegli il nome di dominio. Regione AWS
- Se hai utilizzato account diversi per creare la tua zona ospitata su Route 53 e il tuo dominio di OpenSearch servizio, inserisci il nome di dominio personalizzato. Per ulteriori informazioni, consulta Creare un endpoint personalizzato.

Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare un dominio di OpenSearch servizio, il dominio non verrà visualizzato nell'elenco degli endpoint.

Se hai utilizzato un account per creare la zona ospitata corrente e uno o più account diversi per creare tutti i domini di OpenSearch servizio, l'elenco degli endpoint mostra Nessun obiettivo disponibile in Servizio. OpenSearch

Per ulteriori informazioni, consulta Configurazione di Amazon Route 53 per instradare il traffico verso l'endpoint del dominio Amazon OpenSearch Service.

Endpoint dell'interfaccia di Amazon VPC

Per gli endpoint dell'interfaccia Amazon VPC, effettua una delle seguenti operazioni:

- Se hai usato lo stesso account per creare la zona ospitata Route 53 e l'endpoint dell'interfaccia: scegli Endpoint e seleziona quindi un endpoint dell'interfaccia dall'elenco. Se disponi di molte interfacce di endpoint, puoi inserire i primi caratteri del nome host DNS per filtrare l'elenco.
- Se hai utilizzato account diversi per creare la zona ospitata Route 53 e l'endpoint dell'interfaccia, inserisci il nome host DNS per l'endpoint dell'interfaccia, ad esempio vpce-123456789abcdef01- example-us-east -1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com.

  Se hai utilizzato un AWS account per creare la zona ospitata corrente e un account diverso per creare un endpoint di interfaccia, l'endpoint dell'interfaccia non verrà visualizzato nell'elenco degli endpoint sotto gli endpoint VPC.

  Se hai utilizzato un account per creare la zona ospitata attuale e uno o più account diversi per creare tutti gli endpoint di interfaccia, nell'elenco Endpoint viene visualizzato Nessuna destinazione disponibile in Endpoint VPC.

  Per ulteriori informazioni, consulta Routing del traffico a un endpoint di interfaccia di Amazon Virtual Private Cloud usando il proprio nome dominio.

Record in questa zona ospitata

Per i record in questa zona ospitata, scegli Endpoint, quindi seleziona il record applicabile. Se disponi di molti record, puoi inserire i primi caratteri del nome per filtrare l'elenco.

Se la zona ospitata contiene solo i record NS e SOA di default, nell'elenco Endpoint viene visualizzato Nessuna destinazione disponibile.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi scegliere un record il cui valore di Tipo di record è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valori specifici per record semplici

Quando crei record semplici, specifichi i valori seguenti.

Argomenti

- Policy di routing
- Nome record
- Valore/instradamento traffico a
- Tipo di record
- TTL (secondi)

Policy di routing

Scegli Routing semplice.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Per ulteriori informazioni sui nomi record, consultare Nome record.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo
- AAAA — IPv6 indirizzo

- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- NS - Server di nomi

  Il nome di dominio di un server dei nomi, ad esempio ns1.example.com.

  > **Note**
  >
  > È possibile specificare un record NS con solo una policy di routing.

- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore per Tipo di record in base al modo in cui desideri che Route 53 risponda alle query DNS.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se

stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Valori specifici per record alias semplici

Quando crei record alias, specifichi i valori seguenti. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

> **Note**
>
> Se si utilizza Route 53 in AWS GovCloud (US) Region, questa funzionalità presenta alcune restrizioni. Per ulteriori informazioni, consulta la pagina di Amazon Route 53 nella Guida per l'utente di AWS GovCloud (US) .

Argomenti

- Policy di routing
- Nome record
- Valore/instradamento traffico a
- Tipo di record
- Valutazione dello stato della destinazione

Policy di routing

Scegli Routing semplice.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Per ulteriori informazioni sui nomi record, consultare Nome record.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consulta Common values for alias records for value/indirizzare il traffico verso cui indirizzare il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consulta. Instradamento del traffico Internet verso le tue risorse AWS

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valutazione dello stato della destinazione

Quando il valore di Policy di routing è Semplice, è possibile scegliere tra No il valore di default Sì perché Valuta integrità della destinazione non ha effetto per il routing Semplice. Se hai solo un record con nome e tipo, Route 53 risponde alle query DNS utilizzando i valori in quel record, indipendentemente dall'integrità della risorsa.

Valori specifici per record di failover

Quando crei record di failover, specifichi i valori seguenti.

> **Note**
>
> Per informazioni su come creare record di failover nella propria zona ospitata privata, consulta Configurazione del failover in una zona ospitata privata.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- TTL (secondi)
- Valore/instradamento traffico a
- Tipo di record di failover
- Controllo dello stato
- ID record

Policy di routing

Scegli Failover.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per entrambi i record nel gruppo di record di failover.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona lo stesso valore per i record di failover principali e secondari.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta

- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Tipo di record di failover

Scegli un valore applicabile per questo record. Affinché il failover funzioni correttamente, devi creare un record di failover principale e uno secondario.

Non puoi creare record non di failover che hanno gli stessi valori per Nome record e Tipo di record come record di failover.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come il failover o i record ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate Target Health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su

IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Domain Name (Nome dominio), specifica il nome di dominio del server (ad esempio, us-east-2-www.example.com), anziché il nome dei record (example.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

ID record

Immetti un valore che identifichi in modo univoco i record principale e secondario.

Valori specifici per i record alias di failover

Quando crei record alias di failover, specifichi i valori seguenti.

Per informazioni, consultare gli argomenti seguenti:

- Per informazioni su come creare record di failover nella propria zona ospitata privata, consulta Configurazione del failover in una zona ospitata privata.
- Per ulteriori informazioni sui record alias, consulta Scelta tra record alias e non alias.

Argomenti

Policy di routing

Scegli Failover.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per entrambi i record nel gruppo di record di failover.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico. Seleziona lo stesso valore per i record di failover principali e secondari:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consulta Common values for alias records for value/indirizzare il traffico verso cui indirizzare il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consulta. Instradamento del traffico Internet verso le tue risorse AWS

> **Note**
>
> Quando crei i record di failover principale e secondario, puoi facoltativamente creare un record di failover e un record alias di failover con gli stessi valori per Nome e Tipo di record. Se combini il record di failover con il record alias di failover, entrambi possono essere il record principale.

Tipo di record di failover

Scegli un valore applicabile per questo record. Affinché il failover funzioni correttamente, devi creare un record di failover principale e uno secondario.

Non puoi creare record non di failover che hanno gli stessi valori per Nome record e Tipo di record come record di failover.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come i record di failover o ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate Target Health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Domain Name (Nome dominio), specifica il nome di dominio del server (ad esempio, us-east-2-www.example.com), anziché il nome dei record (example.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate target health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Load Balancer classici: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate target health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/ Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, un gruppo target contenente target deve includere almeno un target integro. Se un gruppo target

contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.

- Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Immetti un valore che identifichi in modo univoco i record principale e secondario.

Valori specifici per record di geolocalizzazione

Quando crei record di geolocalizzazione, specifichi i valori seguenti.

Argomenti

Policy di routing

Seleziona Geolocalizzazione.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Immetti lo stesso nome per tutti i record nel gruppo di record di geolocalizzazione.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona lo stesso valore per tutti i record nel gruppo dei record di geolocalizzazione.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi

- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Ubicazione

Quando configuri Route 53 per rispondere alle query DNS in base alla posizione da cui provengono, seleziona il continente o il paese per il quale desideri che Route 53 risponda con le impostazioni di questo record. Se desideri che Route 53 risponda alle query DNS dei singoli paesi degli Stati Uniti, seleziona Stati Uniti dall'elenco Posizione, quindi seleziona lo stato dal gruppo Posizione secondaria.

Per una zona ospitata privata, seleziona il continente, il paese o la suddivisione più vicina a Regione AWS quella in cui si trova la risorsa. Ad esempio, se la risorsa si trova in us-east-1, puoi specificare Nord America, Stati Uniti o Virginia.

> **Important**
>
> Ti consigliamo di creare un record di geolocalizzazione con il valore Default (Predefinito) per l'opzione Location (Posizione). Questo copre le località geografiche per cui non hai creato record nonché gli indirizzi IP per cui Route 53 non è in grado di identificare una località.

Non puoi creare record di non geolocalizzazione che hanno gli stessi valori per Nome record e Tipo di record come record di geolocalizzazione.

Per ulteriori informazioni, consulta Routing di geolocalizzazione.

Di seguito sono indicati i paesi che Amazon Route 53 associa a ogni continente. I codici dei paesi sono quelli della norma ISO 3166. Per maggiori informazioni, consulta l'articolo di Wikipedia ISO 3166-1 alpha-2:

Africa (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antartide (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

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

Nord America (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oceania (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Sud America (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 non supporta la creazione di record di geolocalizzazione per i seguenti paesi: Isola Bouvet (BV), Isola di Natale (CX), Sahara Occidentale (EH) e Isola e Isole Heard (HM). McDonald Non sono disponibili dati sugli indirizzi IP per questi paesi.

Stati degli Stati Uniti

Quando configuri Route 53 per rispondere alle query DNS in base allo stato degli Stati Uniti da cui provengono, seleziona lo stato dall'elenco Stati degli Stati Uniti. I territori degli Stati Uniti (ad esempio, Porto Rico) sono presenti come paesi nell'elenco Location (Posizione).

Important

Alcuni indirizzi IP sono associati agli Stati Uniti, ma non a un singolo paese. Se crei record per tutti i paesi degli Stati Uniti, ti consigliamo di creare anche un record generico per gli

Stati Uniti per instradare le query per questi indirizzi IP non associati. Se non crei un record generico per gli Stati Uniti, Route 53 risponde alle query DNS provenienti dagli indirizzi IP non associati agli Stati Uniti con le impostazioni del record di geolocalizzazione predefinito (se ne hai creato uno) o con una "non risposta".

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (ad esempio i record di failover o ponderati) e specifichi il controllo dello stato per tutti i record. IDs Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate Target Health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore

di Domain Name (Nome dominio), specifica il nome di dominio del server (ad esempio, us-east-2-www.example.com), anziché il nome dei record (example.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Per i record di geolocalizzazione, se un endpoint non è integro, Route 53 cerca un record per la regione geografica associata più estesa. Ad esempio, supponiamo che siano presenti record per un paese degli Stati Uniti, per tutti gli Stati Uniti, per il Nord America e per tutte le località, con l'opzione Location (Località) impostata su Default (Predefinita). Se l'endpoint per il record del paese non è integro, Route 53 controlla i record per gli Stati Uniti, per il Nord America e per tutte le località, in quest'ordine, finché non trova un record con un endpoint integro. Se tutti i record applicabili sono in uno stato non integro, incluso il record per tutte le sedi, Route 53 risponde a una query DNS con il valore del record della regione geografica più piccola.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record di geolocalizzazione.

Valori specifici per record degli alias di geolocalizzazione

Quando crei record alias di geolocalizzazione, specifichi i valori seguenti.

Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- Valore/instradamento traffico a
- Ubicazione
- Stati degli Stati Uniti
- Controllo dello stato
- Valutazione dello stato della destinazione
- ID record

Policy di routing

Seleziona Geolocalizzazione.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per tutti i record nel gruppo di record di geolocalizzazione.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico. Seleziona lo stesso valore per tutti i record nel gruppo dei record di geolocalizzazione.

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui

stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi rivolgerti, consultaValore/instradamento traffico a.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consultaInstradamento del traffico Internet verso le tue risorse AWS.

Ubicazione

Quando configuri Route 53 per rispondere alle query DNS in base alla posizione da cui provengono, seleziona il continente o il paese per il quale desideri che Route 53 risponda con le impostazioni di questo record. Se desideri che Route 53 risponda alle query DNS dei singoli stati degli Stati Uniti, seleziona Stati Uniti dall'elenco Posizione, quindi seleziona lo stato dall'elenco Stati degli Stati Uniti.

Per una zona ospitata privata, seleziona il continente, il paese o la suddivisione più vicina a Regione AWS quella in cui si trova la risorsa. Ad esempio, se la risorsa si trova in us-east-1, puoi specificare Nord America, Stati Uniti o Virginia.

Important

Ti consigliamo di creare un record di geolocalizzazione con il valore Default (Predefinito) per l'opzione Location (Posizione). Questo copre le località geografiche per cui non hai creato record nonché gli indirizzi IP per cui Route 53 non è in grado di identificare una località.

Non puoi creare record di non geolocalizzazione che hanno gli stessi valori per Nome record e Tipo di record come record di geolocalizzazione.

Per ulteriori informazioni, consulta Routing di geolocalizzazione.

Di seguito sono indicati i paesi che Amazon Route 53 associa a ogni continente. I codici dei paesi sono quelli della norma ISO 3166. Per maggiori informazioni, consulta l'articolo di Wikipedia ISO 3166-1 alpha-2:

Africa (AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

Antartide (AN)

AQ, GS, TF

Asia (AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

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

Nord America (NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

Oceania (OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

Sud America (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

Route 53 non supporta la creazione di record di geolocalizzazione per i seguenti paesi: Isola Bouvet (BV), Isola di Natale (CX), Sahara Occidentale (EH) e Isola e Isole Heard (HM). McDonald Non sono disponibili dati sugli indirizzi IP per questi paesi.

Stati degli Stati Uniti

Quando configuri Route 53 per rispondere alle query DNS in base allo stato degli Stati Uniti da cui provengono, seleziona lo stato dall'elenco Stati degli Stati Uniti. I territori degli Stati Uniti (ad esempio, Porto Rico) sono presenti come paesi nell'elenco Location (Posizione).

> **Important**
>
> Alcuni indirizzi IP sono associati agli Stati Uniti, ma non a un singolo paese. Se crei record per tutti i paesi degli Stati Uniti, ti consigliamo di creare anche un record generico per gli Stati Uniti per instradare le query per questi indirizzi IP non associati. Se non crei un record generico per gli Stati Uniti, Route 53 risponde alle query DNS provenienti dagli indirizzi IP non associati agli Stati Uniti con le impostazioni del record di geolocalizzazione predefinito (se ne hai creato uno) o con una "non risposta".

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (ad esempio i record di failover o ponderati) e specifichi il controllo dello stato per tutti i record. IDs Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona

ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Per i record di geolocalizzazione, se un endpoint non è integro, Route 53 cerca un record per la regione geografica associata più estesa. Ad esempio, supponiamo che siano presenti record per un paese degli Stati Uniti, per tutti gli Stati Uniti, per il Nord America e per tutte le località, con l'opzione Location (Località) impostata su Default (Predefinita). Se l'endpoint per il record del paese non è integro, Route 53 controlla i record per gli Stati Uniti, per il Nord America e per tutte le località, in quest'ordine, finché non trova un record con un endpoint integro. Se tutti i record applicabili sono in uno stato non integro, incluso il record per tutte le sedi, Route 53 risponde a una query DNS con il valore del record della regione geografica più piccola.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate target health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Classic Load Balancer: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate target health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, ogni gruppo target contenente target deve includere almeno un target integro. Se un gruppo target contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.
  - Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record di geolocalizzazione.

Valori specifici per i record di geoprossimità

Quando si creano record di geoprossimità, si specificano i seguenti valori.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- TTL (secondi)
- Valore/instradamento traffico a
- Endpoint location (Posizione endpoint)
- Bias
- Controllo dello stato
- ID record

Policy di routing

Scegli Geoproximity.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Inserisci lo stesso nome per tutti i record del gruppo di record di geoprossimità.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona lo stesso valore per tutti i record del gruppo di record di geoprossimità.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — indirizzo IPv4
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi

- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Endpoint location (Posizione endpoint)

È possibile specificare la posizione dell'endpoint della risorsa utilizzando uno dei seguenti metodi:

Coordinate personalizzate

Specificare la longitudine e la latitudine per un'area geografica.

Regione AWS

Scegliete una regione disponibile dall'elenco delle località.

Per ulteriori informazioni sulle regioni, consulta Infrastruttura AWS globale.

AWS Gruppo di zone locali

Scegliete un gruppo di zone locali disponibile dall'elenco delle ubicazioni.

Per ulteriori informazioni sulle Local Zones, vedere Available Local Zones nella AWS Local Zones User Guide. Un gruppo di zone locale è in genere la zona locale senza il carattere finale. Ad esempio, se la zona locale è, `us-east-1-bue-1a` il gruppo di zone locali lo è`us-east-1-bue-1`.

Puoi anche identificare il Local Zones Group per una zona locale specifica utilizzando il comando describe-availability-zonesCLI:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Questo comando restituisce:`"GroupName": "us-west-2-den-1"`, specificando che la zona locale `us-west-2-den-1a` appartiene al gruppo di zone locali. `us-west-2-den-1`

Non è possibile creare record non di geoprossimità con gli stessi valori per Record name e Record type dei record di geoprossimità.

Inoltre, non è possibile creare due set di record di risorse di geoprossimità che specificano la stessa posizione per lo stesso nome e tipo di record.

Bias

Una distorsione espande o riduce un'area geografica da cui la Route 53 indirizza il traffico verso una risorsa. Un bias positivo amplia l'area, mentre un bias negativo la restringe. Per ulteriori informazioni, consulta Come Amazon Route 53 utilizza il bias per instradare il traffico.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Si verifica lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e politica di routing (ad esempio i record di failover o ponderati) e si specifica il controllo dello stato per tutti i record. IDs Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Si seleziona Sì per Evaluate Target Health per un record di alias o per i record in un gruppo di alias di failover, alias di geolocalizzazione, alias di geoprossimità, alias di latenza, alias basato su IP o record di alias ponderato. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Domain Name (Nome dominio), specifica il nome di dominio del server (ad esempio, us-east-2-www.example.com), anziché il nome dei record (example.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Per i record di geoprossimità, se un endpoint non è integro, Route 53 cerca un endpoint più vicino che sia ancora integro.

ID record

Inserisci un valore che identifichi in modo univoco questo record nel gruppo di record di geoprossimità.

Valori specifici per i record di alias di geoprossimità

Quando si creano record di alias di geoprossimità, si specificano i seguenti valori.

Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- Valore/instradamento traffico a
- Endpoint location (Posizione endpoint)
- Bias
- Controllo dello stato
- Valutazione dello stato della destinazione
- ID record

Policy di routing

Scegli Geoproximity.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Inserisci lo stesso nome per tutti i record del gruppo di record di geoprossimità.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico. Seleziona lo stesso valore per tutti i record del gruppo di record di geoprossimità:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui

stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consultaValore/instradamento traffico a.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consultaInstradamento del traffico Internet verso le tue risorse AWS.

Endpoint location (Posizione endpoint)

È possibile specificare la posizione dell'endpoint della risorsa utilizzando uno dei seguenti metodi:

Coordinate personalizzate

Specificare la longitudine e la latitudine per un'area geografica.

Regione AWS

Scegliete una regione disponibile dall'elenco delle località.

Per ulteriori informazioni sulle regioni, consulta Infrastruttura AWS globale.

AWS Gruppo di zone locali

Scegliete una regione di zona locale disponibile dall'elenco delle ubicazioni.

Per ulteriori informazioni sulle Local Zones, vedere Available Local Zones nella AWS Local Zones User Guide. Un gruppo di zone locale è in genere la zona locale senza il carattere finale. Ad esempio, se la zona locale è, `us-east-1-bue-1a` il gruppo di zone locali lo è`us-east-1-bue-1`.

Puoi anche identificare il Local Zones Group per una zona locale specifica utilizzando il comando describe-availability-zonesCLI:

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

Questo comando restituisce:`"GroupName": "us-west-2-den-1"`, specificando che la zona locale `us-west-2-den-1a` appartiene al gruppo di zone locali. `us-west-2-den-1`

Non è possibile creare record non di geoprossimità con gli stessi valori per Record name e Record type dei record di geoprossimità.

Inoltre, non è possibile creare due set di record di risorse di geoprossimità che specificano la stessa posizione per lo stesso nome e tipo di record.

Per ulteriori informazioni, consulta .html available-local-zones

Bias

Una distorsione espande o riduce un'area geografica da cui la Route 53 indirizza il traffico verso una risorsa. Un bias positivo amplia l'area, mentre un bias negativo la restringe. Per ulteriori informazioni, consulta Come Amazon Route 53 utilizza il bias per instradare il traffico.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Si verifica lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e politica di routing (ad esempio i record di failover o ponderati) e si specifica il controllo dello stato per tutti i record. IDs Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Si seleziona Sì per Valutare lo stato dell'obiettivo per un record di alias o per i record in un gruppo di alias di failover, alias di geolocalizzazione, alias di geoprossimità, alias di latenza, alias basato

su IP o record di alias ponderato. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Per i record di geoprossimità, se un endpoint non è integro, Route 53 cerca un endpoint più vicino che sia ancora integro.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate target health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Classic Load Balancer: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate target health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, ogni gruppo target contenente target deve includere almeno un target integro. Se un gruppo target contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.
  - Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Inserisci un valore che identifichi in modo univoco questo record nel gruppo di record di geoprossimità.

Valori specifici per i record di latenza

Quando crei record di latenza, specifichi i valori seguenti.

Argomenti

Policy di routing

Scegli Latenza.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per tutti i record nel gruppo di record di latenza.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Selezionare il valore di Tipo in base al modo in cui si desidera che Route 53 risponda alle query DNS.

Seleziona lo stesso valore per tutti i record nel gruppo di record di latenza.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework

- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Regione

La EC2 regione Amazon in cui risiede la risorsa specificata in questo record. Route 53 consiglia una EC2 regione Amazon in base ad altri valori che hai specificato. Lo stesso vale anche per le zone ospitate private. Ti consigliamo di non modificare questo valore.

Tieni presente quanto segue:

- Puoi creare un solo record di latenza per ogni EC2 regione Amazon.
- Non è necessario creare record di latenza per tutte le EC2 regioni Amazon. Route 53 sceglie la regione con la migliore latenza tra quelle per cui hai creato i record di latenza.
- Non puoi creare record di non latenza che hanno gli stessi valori per Nome record e Tipo di record come record di latenza.
- Se crei un record con il tag della regione cn-north-1, Route 53 risponde sempre alle query provenienti dalla Cina utilizzando questo record, indipendentemente dalla latenza.

Per ulteriori informazioni sull'utilizzo dei record di latenza, consulta Routing basato sulla latenza.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come i record di failover o ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record di latenza.

Valori specifici per i record alias di latenza

Quando crei record alias di latenza, specifichi i valori seguenti.

Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- Valore/instradamento traffico a
- Regione
- Controllo dello stato
- Valutazione dello stato della destinazione
- ID record

Policy di routing

Scegli Latenza.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per tutti i record nel gruppo di record di latenza.

Per ulteriori informazioni sui nomi dei record, consultare Nome record

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Seleziona lo stesso valore per tutti i record nel gruppo di record di latenza.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consulta Common values for alias records for value/indirizzare il traffico verso cui indirizzare il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consulta. Instradamento del traffico Internet verso le tue risorse AWS

Regione

La EC2 regione Amazon in cui risiede la risorsa specificata in questo record. Route 53 consiglia una EC2 regione Amazon in base ad altri valori che hai specificato. Lo stesso vale anche per le zone ospitate private. Ti consigliamo di non modificare questo valore.

Tieni presente quanto segue:

- Puoi creare un solo record di latenza per ogni EC2 regione Amazon.
- Non è necessario creare record di latenza per tutte le EC2 regioni Amazon. Route 53 sceglie la regione con la migliore latenza tra quelle per cui hai creato i record di latenza.
- Non puoi creare record di non latenza che hanno gli stessi valori per Nome record e Tipo di record come record di latenza.
- Se crei un record con il tag della regione cn-north-1, Route 53 risponde sempre alle query provenienti dalla Cina utilizzando questo record, indipendentemente dalla latenza.

Per ulteriori informazioni sull'utilizzo dei record di latenza, consulta Routing basato sulla latenza.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per

un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come i record di failover o ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate Target Health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Classic Load Balancer: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate target health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/ Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, ogni gruppo target contenente target deve includere almeno un target integro. Se un gruppo target contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.
  - Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record di latenza.

Valori specifici per i record basati su IP

Quando crei i record basati su IP, specifica i valori seguenti.

> **Note**
>
> Sebbene la creazione di record basati su IP in una zona ospitata privata sia consentita, non è supportata.

Argomenti

Policy di routing

Scegli IP-based (Basato su IP).

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Inserisci lo stesso nome per tutti i record nel gruppo di record basati su IP.

Registri CNAME

Se stai creando un record che ha lo stesso valore di CNAME per Tipo di record, il nome del record non può essere uguale al nome della zona ospitata.

Caratteri speciali

Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

Caratteri jolly

Puoi utilizzare un asterisco (*) all'interno del nome. Il DNS considera il carattere * sia come un carattere jolly che come il carattere * (ASCII 42), a seconda della posizione nel nome. Per ulteriori informazioni, consulta Utilizza un asterisco (*) nei nomi di zone ospitate e registri.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Selezionare il valore di Tipo in base al modo in cui si desidera che Route 53 risponda alle query DNS.

Seleziona lo stesso valore per tutti i record del gruppo di record basati su IP.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — indirizzo IPv4
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i Valore/instradamento traffico a valori comuni per Valore/instradamento traffico a.

Ubicazione

Il nome della posizione CIDR in cui la risorsa indicata in questo record è specificata dai valori del blocco CIDR all'interno della posizione.

Per ulteriori informazioni sull'utilizzo dei record basati su IP, consulta Routing basato su IP.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per

informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come il failover o i record ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valuta integrità destinazione) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, basati su IP, di latenza o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

ID record

Inserisci un valore che identifichi in modo univoco questo record nel gruppo di record basati su IP.

Valori specifici per i record alias basati su IP

Quando crei record alias basati su IP, specifica i valori seguenti.

> **Note**
>
> Sebbene la creazione di record alias basati su IP in una zona ospitata privata sia consentita, non è supportata.

Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- Valore/instradamento traffico a
- Ubicazione
- Controllo dello stato
- Valutazione dello stato della destinazione
- ID record

Policy di routing

Scegli IP-based (Basato su IP).

> **Note**
>
> Sebbene la creazione di record alias basati su IP in una zona ospitata privata sia consentita, non è supportata.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Inserisci lo stesso nome per tutti i record nel gruppo di record basati su IP.

Registri CNAME

Se stai creando un record che ha lo stesso valore di CNAME per Tipo di record, il nome del record non può essere uguale al nome della zona ospitata.

Alias per CloudFront distribuzioni e bucket Amazon S3

Il valore specificato dipende in parte dalla AWS risorsa verso cui stai instradando il traffico:

- CloudFront distribuzione: la distribuzione deve includere un nome di dominio alternativo che corrisponda al nome del record. Ad esempio, se il nome del record è acme.example.com, la distribuzione CloudFront deve includere acme.example.com come uno dei nomi di dominio alternativi. Per ulteriori informazioni, consulta Using alternate domain names (CNAMEs) nella Amazon CloudFront Developer Guide.
- Bucket Amazon S3: il nome del record deve corrispondere al nome del bucket Amazon S3. Ad esempio, se il nome del bucket è acme.example.com, anche il nome del record deve essere acme.example.com.

  Inoltre, devi configurare il bucket per l'hosting di siti Web. Per ulteriori informazioni, consulta Configurazione di un bucket per l'hosting di un sito Web nella Guida per utenti di Amazon Simple Storage Service.

Caratteri speciali

Per informazioni su come specificare caratteri diversi da a-z, 0-9 e - (trattino) e come specificare nomi di dominio internazionali, consulta Formato del nome dominio DNS.

Caratteri jolly

Puoi utilizzare un asterisco (*) all'interno del nome. Il DNS considera il carattere * sia come un carattere jolly che come il carattere * (ASCII 42), a seconda della posizione nel nome. Per ulteriori informazioni, consulta Utilizza un asterisco (*) nei nomi di zone ospitate e registri.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico. Seleziona lo stesso valore per tutti i record nel gruppo di record basati su IP:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consulta Common values for alias records for value/indirizzare il traffico verso cui indirizzare il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consulta. Instradamento del traffico Internet verso le tue risorse AWS

Ubicazione

Quando configuri Route 53 per rispondere alle query DNS in base alla posizione da cui provengono, seleziona la posizione CIDR per la quale desideri che Route 53 risponda con le impostazioni di questo record.

> **Important**
>
> Ti consigliamo di creare un record basato su IP con il valore Default (Predefinito) per l'opzione Location (Posizione). Questo copre le posizioni per cui non hai creato i record nonché gli indirizzi IP per cui Route 53 non è in grado di identificare una posizione.

Non è possibile creare non-IP-based record con gli stessi valori per Nome record e Tipo di record dei record basati su IP.

Per ulteriori informazioni, consulta Routing basato su IP.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (ad esempio il failover o i record ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valuta integrità destinazione) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, ponderati o alias di routing basati su IP. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Per i record di alias basati su IP, se un endpoint non è integro, Route 53 cerca un record all'interno della posizione associata più grande. Ad esempio, supponiamo che siano presenti record per un paese degli Stati Uniti, per tutti gli Stati Uniti, per il Nord America e per tutte le località, con l'opzione Location (Località) impostata su Default (Predefinita). Se l'endpoint per il record del paese non è integro, Route 53 controlla i record per gli Stati Uniti, per il Nord America e per tutte le località, in quest'ordine, finché non trova un record con un endpoint integro. Se tutti i record applicabili sono in uno stato non integro, incluso il record per tutte le sedi, Route 53 risponde a una query DNS con il valore del record della regione geografica più piccola.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate target health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza

Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Classic Load Balancer: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate target health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, ogni gruppo target contenente target deve includere almeno un target integro. Se un gruppo target contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.
  - Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Inserisci un valore che identifichi in modo univoco questo record nel gruppo di record basati su IP.

Valori specifici per record di risposta multivalore

Quando crei record di risposta multivalore, specifichi i valori seguenti.

> **Note**
>
> La creazione di record alias di risposta multivalore non è supportata.

Argomenti

Policy di routing

Scegli Risposta multivalore.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per tutti i record nel gruppo di record multivalore.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona qualsiasi valore ad eccezione di NS o CNAME.

Seleziona lo stesso valore per tutti i record nel gruppo di record di risposta multivalore.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

> **Note**
>
> Se crei due o più record di risposta multivalore con lo stesso nome e tipo, stai utilizzando la consolle e se specifichi diversi valori per TTL, Route 53 modifica il valore di TTL per tutti i record impostandolo sull'ultimo valore specificato.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Quando inserisci più di un valore, inserisci ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo
- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come il failover o i record ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Selezioni Sì per Valutazione dell'integrità della destinazione per un record alias o i record in un gruppo di alias di failover, alias di geolocalizzazione, alias di latenza o alias ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo

dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

ID record

Immetti un valore che identifica in modo univoco questo record nel gruppo di record di risposta multivalore.

Valori specifici per record ponderati

Quando crei record ponderati, specifichi i valori seguenti.

Argomenti

Policy di routing

Selezionare Weighted (Ponderato).

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Nome record.

Immetti lo stesso nome per tutti i record nel gruppo di record ponderati.

Per ulteriori informazioni sui nomi record, consultare Nome record.

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona lo stesso valore per tutti i record nel gruppo dei record ponderati.

TTL (secondi)

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore più lungo (ad esempio, 172800 secondi o due giorni), riduci il numero di chiamate che i resolver ricorsivi DNS devono eseguire per permettere a Route 53 di ottenere le informazioni più recenti in questo record. Ciò ha l'effetto di ridurre la latenza e i costi per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Tuttavia, se specifichi un valore più lungo per TTL, è necessario più tempo perché le modifiche al record (ad esempio, un nuovo indirizzo IP) abbiano effetto in quanto i resolver ricorsivi utilizzano i valori nella cache per periodi più lunghi prima di chiedere a Route 53 le informazioni più recenti. Se stai modificando le impostazioni per un dominio o sottodominio che è già in uso, ti consigliamo di specificare inizialmente un valore più breve, ad esempio 300 secondi, e aumentare il valore dopo aver verificato che le nuove impostazioni siano corrette.

Se stai associando questo record a un controllo dell'integrità, ti consigliamo di specificare un TTL di 60 secondi o inferiore in modo che i client rispondano rapidamente alle modifiche dello stato.

Devi specificare lo stesso valore TTL per tutti i record di questo gruppo di record ponderati.

> **Note**
>
> Se crei due o più record ponderati con lo stesso nome e tipo e specifichi diversi valori TTL, Route 53 modifica il valore TTL per tutti i record utilizzando l'ultimo valore specificato.

Se un gruppo di record ponderati include uno o più record alias ponderati che instradano il traffico a un load balancer ELB, ti consigliamo di specificare un TTL di 60 secondi per tutti i record non alias ponderati che hanno lo stesso nome e tipo. I valori diversi da 60 secondi (TTL per sistemi di bilanciamento del carico) modificheranno l'effetto dei valori che specifichi per Weight (Peso).

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record. Immetti un valore appropriato per il valore di Tipo di record. Per tutti i tipi ad eccezione di CNAME, puoi immettere più di un valore. Immetti ogni valore su una riga distinta.

Puoi instradare il traffico verso, o specificare i seguenti valori:

- A — IPv4 indirizzo

- AAAA — IPv6 indirizzo
- CAA - Autorizzazione della certification authority
- CNAME - Nome canonico
- MX - Scambio di posta
- NAPTR - Puntatore dell'autorità dei nomi
- PTR - Puntatore
- SPF - Sender Policy Framework
- SRV - Localizzatore di servizi
- TXT - Testo

Per ulteriori informazioni su questi valori, consulta i valori comuni per Valore/instradamento traffico a.

Weight

Un valore che determina la proporzione di query DNS a cui Route 53 risponde utilizzando il record corrente. Route 53 calcola la somma dei pesi per i record che hanno la stessa combinazione di tipo e nome DNS. Route 53 risponde quindi alle query in base alla proporzione tra il peso di una risorsa e il totale.

Non puoi creare record non ponderati che hanno gli stessi valori per Nome record e Tipo di record come record ponderati.

Immetti un intero compreso tra 0 e 255. Per disattivare il routing a una risorsa, imposta Weight (Peso) su 0. Se imposti Weight (Peso) su 0 per tutti i record nel gruppo, il traffico viene instradato a tutte le risorse con una probabilità equivalente. Ciò impedisce la disattivazione accidentale del routing per un gruppo di record ponderati.

L'effetto di impostare Weight (Peso) su 0 è differente quando associ controlli dell'integrità a record ponderati. Per ulteriori informazioni, consulta Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per

un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come il failover o i record ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record ponderati.

Valori specifici per i record alias ponderati

Quando crei record alias ponderati, specifichi i valori seguenti. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Argomenti

- Policy di routing
- Nome record
- Tipo di record
- Valore/instradamento traffico a
- Weight
- Controllo dello stato
- Valutazione dello stato della destinazione
- ID record

Policy di routing

Scegli Ponderata.

Nome record

Immetti il nome del dominio o sottodominio a cui instradare il traffico. Il valore predefinito è il nome della hosted zone.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Immetti lo stesso nome per tutti i record nel gruppo di record ponderati.

Per ulteriori informazioni sui nomi dei record, consultare Nome record

Tipo di record

Il tipo di record DNS. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Seleziona il valore applicabile in base alla AWS risorsa verso cui stai indirizzando il traffico:

API regionali personalizzate di API Gateway o API con ottimizzate per l'edge

Seleziona A — IPv4 indirizzo.

Endpoint dell'interfaccia di Amazon VPC

Seleziona A — IPv4 indirizzo.

CloudFront distribuzione

Seleziona A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione, crea due record, uno con il valore A - IPv4 indirizzo per Tipo e uno con il valore AAAA - IPv6 indirizzo.

Servizio App Runner

Seleziona A — indirizzo IPv4

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Seleziona A — IPv4 indirizzo

Sistema di bilanciamento del carico ELB

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Bucket Amazon S3

Seleziona A — indirizzo IPv4

OpenSearch Servizio

Seleziona A — IPv4 indirizzo o AAAA — IPv6 indirizzo

Un altro record si trova in questa zona ospitata

Seleziona il tipo di record per cui stai creando l'alias. Sono supportati tutti i tipi a eccezione di NS e SOA.

> **Note**
>
> Se stai creando un record alias che ha lo stesso valore della zona ospitata (nota come Apex di zona), non puoi instradare il traffico verso un record il cui valore di Type (Tipo) è CNAME. Questo perché il record alias deve avere lo stesso tipo del record a cui stai instradando il traffico e la creazione di un record CNAME per l'apex di zona non è supportata neanche per un record alias.

Seleziona lo stesso valore per tutti i record nel gruppo dei record ponderati.

Valore/instradamento traffico a

Il valore che scegli dall'elenco o che digiti nel campo dipende dalla AWS risorsa verso cui stai indirizzando il traffico.

Per informazioni sulle AWS risorse a cui puoi indirizzare, consulta Common values for alias records for value/indirizzare il traffico verso cui indirizzare il traffico.

Per ulteriori informazioni su come configurare Route 53 per indirizzare il traffico verso AWS risorse specifiche, consulta. Instradamento del traffico Internet verso le tue risorse AWS

Weight

Un valore che determina la proporzione di query DNS a cui Route 53 risponde utilizzando il record corrente. Route 53 calcola la somma dei pesi per i record che hanno la stessa combinazione di tipo e nome DNS. Route 53 risponde quindi alle query in base alla proporzione tra il peso di una risorsa e il totale.

Non puoi creare record non ponderati che hanno gli stessi valori per Nome record e Tipo di record come record ponderati.

Immetti un intero compreso tra 0 e 255. Per disattivare il routing a una risorsa, imposta Weight (Peso) su 0. Se imposti Weight (Peso) su 0 per tutti i record nel gruppo, il traffico viene instradato a tutte le risorse con una probabilità equivalente. Ciò impedisce la disattivazione accidentale del routing per un gruppo di record ponderati.

L'effetto di impostare Weight (Peso) su 0 è differente quando associ controlli dell'integrità a record ponderati. Per ulteriori informazioni, consulta Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità.

Controllo dello stato

Seleziona un controllo dell'integrità se desideri che Route 53 controlli l'integrità di un determinato endpoint e risponda alle query DNS utilizzando questo record solo quando l'endpoint è integro.

Route 53 non controlla l'integrità dell'endpoint specificato nel record, ad esempio l'endpoint specificato dall'indirizzo IP nel campo Valore. Quando selezioni un controllo dell'integrità per un record, Route 53 controlla l'integrità dell'endpoint specificato nel controllo dell'integrità. Per

informazioni su come Route 53 determina se un endpoint è integro, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

L'associazione di un controllo dell'integrità a un record è utile solo quando Route 53 deve scegliere tra due o più record per rispondere a una query DNS e desideri che Route 53 effettui la scelta in parte in base all'avanzamento di un controllo dell'integrità. Utilizza i controlli dell'integrità solo nelle configurazioni seguenti:

- Stai controllando lo stato di tutti i record di un gruppo di record con lo stesso nome, tipo e policy di routing (come i record di failover o ponderati) e specifichi il controllo dello stato IDs per tutti i record. Se il controllo dell'integrità di un record indica un endpoint non integro, Route 53 smette di rispondere alle query utilizzando il valore di tale record.
- Seleziona Yes (Sì) per l'opzione Evaluate target health (Valutazione dello stato target) per un record alias o per i record di un gruppo di alias di failover, di geolocalizzazione, di latenza, basati su IP o ponderati. Se i record alias fanno riferimento a record non alias appartenenti alla stessa zona ospitata, devi specificare anche i controlli dell'integrità per i record a cui viene fatto riferimento. Se associ un controllo dell'integrità a un record alias e selezioni anche Yes (Sì) per Evaluate Target Health (Valuta integrità destinazione), entrambi devono essere veri. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.

Se i controlli dell'integrità specificano l'endpoint solo in base al nome del dominio, ti consigliamo di creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Come valore di Nome dominio, specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Valutazione dello stato della destinazione

Seleziona Sì se desideri che Route 53 determini se rispondere alle query DNS utilizzando questo record controllando l'integrità della risorsa specificata da Endpoint.

Tieni presente quanto segue:

API Gateway personalizzato, regionale APIs e ottimizzato per l'edge APIs

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un'API regionale personalizzata di API Gateway o un'API ottimizzata per l'edge.

CloudFront distribuzioni

Non è possibile impostare Evaluate target health su Sì quando l'endpoint è una CloudFront distribuzione.

Ambienti Elastic Beanstalk con sottodomini regionalizzati

Se specifichi un ambiente Elastic Beanstalk in Endpoint e l'ambiente contiene un load balancer ELB, Elastic Load Balancing indirizza le query solo alle istanze Amazon integre registrate con il EC2 load balancer. (Un ambiente contiene automaticamente un load balancer ELB se include più di un' EC2 istanza Amazon.) Se imposti Evaluate target health su Sì e nessuna EC2 istanza Amazon è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse disponibili che sono integre, se presenti.

Se l'ambiente contiene una singola EC2 istanza Amazon, non ci sono requisiti speciali.

Load balancer ELB

Il comportamento del controllo dell'integrità dipende dal tipo di load balancer:

- Classic Load Balancer: se specifichi un ELB Classic Load Balancer in Endpoint, Elastic Load Balancing indirizza le query solo alle istanze EC2 Amazon integre registrate con il load balancer. Se imposti Evaluate Target Health su Sì e nessuna EC2 istanza è integra o il load balancer stesso non è integro, Route 53 indirizza le query ad altre risorse.
- Application Load Balancer/Network Load Balancer: se specifichi un Application Load Balancer/ Network Load Balancer ELB e imposti Valutazione dell'integrità della destinazione su Sì, Route 53 instrada le query al load balancer in base all'integrità dei gruppi di destinazione a esso associati:
  - Affinché un Application Load Balancer/Network Load Balancer venga considerato integro, ogni gruppo target contenente target deve includere almeno un target integro. Se un gruppo target contiene solo target non integri, il load balancer viene considerato non integro e Route 53 instrada le query ad altre risorse.
  - Un gruppo target che non include target registrati viene considerato non integro.

> **Note**
>
> Quando crei un load balancer, configuri le impostazioni per i controlli dell'integrità di Elastic Load Balancing, che svolgono una funzione analoga ai controlli dell'integrità di Route 53. Non create controlli di integrità di Route 53 per EC2 le istanze registrate con un sistema di bilanciamento del carico ELB.

Bucket S3

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un bucket S3.

Endpoint dell'interfaccia di Amazon VPC

Non sono previsti requisiti speciali per impostare Valutazione dell'integrità della destinazione su Sì quando l'endpoint è un endpoint dell'interfaccia Amazon VPC.

Altri record nella stessa zona ospitata

Se la AWS risorsa specificata in Endpoint è un record o un gruppo di record (ad esempio, un gruppo di record ponderati) ma non è un altro record di alias, ti consigliamo di associare un controllo dello stato a tutti i record dell'endpoint. Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

ID record

Immetti un valore che identifichi in modo univoco questo record nel gruppo di record ponderati.

Creazione di record mediante importazione di un file di zona

Se esegui la migrazione da un altro fornitore di servizi DNS, e se il tuo attuale fornitore di servizi DNS consente di esportare le impostazioni DNS correnti a un file di zona, puoi creare rapidamente tutti i record per una zona ospitata di Amazon Route 53 tramite l'importazione di un file di zona.

> **Note**
>
> Un file di zona utilizza un formato standard noto come BIND per rappresentare i record in un formato di testo. Per ulteriori informazioni sul formato di un file di zona, consulta la voce Wikipedia relativa ai file di zona. Ulteriori informazioni sono disponibili in RFC 1034,

Nomi di dominio - Concetti e funzionalità sezione 3.6.1 e RFC 1035, Nome di dominio - Implementazione e specifica sezione 5.

Se desideri creare record importando un file di zona, tieni presente quanto segue:

- Il file di zona deve essere in formato conforme a RFC.
- Il nome di dominio dei record nel file di zona deve corrispondere al nome della zona ospitata.
- Route 53 supporta le parole chiave `$ORIGIN` e `$TTL`. Se il file di zona include parole chiave `$GENERATE` o `$INCLUDE`, l'importazione ha esito negativo e Route 53 restituisce un errore.
- Quando importi il file di zona, Route 53 ignora il record SOA nel file di zona. Route 53 ignora inoltre qualsiasi record NS che ha lo stesso nome della zona ospitata.
- Puoi importare un massimo di 1.000 record.
- Se la zona ospitata contiene già record visualizzati nel file di zona, il processo di importazione ha esito negativo e non viene creato alcun record.
- Ti consigliamo di esaminare i contenuti del file di zona per verificare che i nomi dei record includano o escludano un punto finale come appropriato:
  - Quando il nome di un record nel file di zona include un punto finale (`example.com.`), il processo di importazione interpreta il nome come nome di dominio completo e crea un record Route 53 con questo nome.
  - Quando il nome di un record nel file di zona non include un punto finale (`www`), il processo di importazione concatena il nome con il nome di dominio nel file di zona (`example.com`) e crea un record Route 53 con il nome concatenato (`www.example.com`).

  Il processo di esportazione non aggiunge un punto finale ai nomi di dominio completi di un record, perciò il processo di importazione di Route 53 aggiunge il nome di dominio al nome del record. Supponiamo ad esempio di importare record nella zona ospitata `example.com` e il nome di un record MX nel file di zona è `mail.example.com`, senza punto finale. Il processo di importazione di Route 53 crea un record MX denominato `mail.example.com.example.com`.

> **Important**
>
> Per i record CNAME, MX, PTR e SRV, questo comportamento, inoltre, è valido per il nome di dominio che è incluso nel valore RDATA. Supponiamo ad esempio che tu abbia un file di zona per `example.com`. Se un record CNAME nel file di zona (`support`, senza un punto finale) ha un valore RDATA di `www.example.com` (anch'esso senza un punto finale), il

processo di importazione crea un record Route 53 con il nome `support.example.com` che consente di instradare il traffico a `www.example.com.example.com`. Prima di importare il tuo file di zona, rivedi i valori RDATA e aggiornali come applicabile.

Route 53 non supporta l'esportazione di record a un file di zona.

> **Note**
>
> Se stai creando un record con lo stesso nome della zona ospitata, non immettere un valore (ad esempio, il simbolo @) nel campo Name (Nome).

Come creare record mediante importazione di un file di zona

1. Ottieni un file di zona dal fornitore di servizi DNS che serve attualmente il dominio. Il processo e la terminologia variano da un fornitore di servizi all'altro. Fai riferimento all'interfaccia del fornitore e alla relativa documentazione per informazioni sull'esportazione o il salvataggio dei record in un file di zona o un file BIND.

   Se il processo non è ovvio, prova a chiedere al servizio di assistenza clienti del tuo attuale fornitore di DNS informazioni su elenco di record o file di zona.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Nella pagina Zone ospitate, crea una nuova zona ospitata:
   a. Scegli Crea zona ospitata.
   b. Inserisci il nome del tuo dominio e, facoltativamente, un commento.
   c. Scegli Create (Crea) .
5. Scegli Importa file di zona.
6. Nel riquadro Importa file di zona, incolla il contenuto del file di zona nella casella di testo File di zona.
7. Seleziona Importa.

> **Note**
>
> A seconda del numero di record nel file di zona, potrebbe essere necessario attendere alcuni minuti prima che vengano creati i record.

8. Se usi un altro servizio DNS per il dominio (cosa comune se hai registrato il dominio con un altro registrar), migra il servizio DNS a Route 53. Al termine di questa fase, il tuo registrar inizierà a identificare Route 53 come servizio DNS in risposta alle query DNS per il tuo dominio e le query inizieranno a essere inviate ai server DNS di Route 53. (Normalmente, ci sono uno o due giorni di ritardo prima che le query DNS vengano instradate a Route 53 perché le informazioni sul servizio DNS precedente sono memorizzate nella cache nel resolver DNS per quel periodo.) Per ulteriori informazioni, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Modifica di record

La procedura seguente spiega come modificare i record utilizzando la console Amazon Route 53. Per informazioni su come modificare i record utilizzando l'API Route 53, consulta ChangeResourceRecordSetsAmazon Route 53 API Reference.

> **Note**
>
> Le modifiche ai registri richiedono tempo per propagarsi ai server DNS di Route 53. Attualmente, l'unico modo per verificare che le modifiche si siano propagate è utilizzare l'azione GetChangeAPI. In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Come modificare i record utilizzando la console Route 53

1. Se non stai modificando record alias, passa al punto 2.

   Se stai modificando record alias che instradano il traffico a Classic Load Balancer, Application Load Balancer o Network Load Balancer Elastic Load Balancing e se hai creato la zona ospitata Route 53 e il sistema di bilanciamento del carico utilizzando account diversi, esegui la procedura Come ottenere il nome DNS per un sistema di bilanciamento del carico Elastic Load Balancing per ottenere il nome DNS per il sistema di bilanciamento del carico.

Se stai modificando i record di alias per qualsiasi altra AWS risorsa, vai al passaggio 2.

2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Nella pagina Hosted Zones (Zone ospitate), scegliere la riga per la zona ospitata che contiene i record che da modificare.
5. Seleziona la riga per il record da modificare e immetti le modifiche nel riquadro Modifica record.
6. Immetti i valori applicabili. Per ulteriori informazioni, consulta Di seguito sono descritti i valori che devi specificare durante la creazione o la modifica di record di Amazon Route 53..
7. Scegli Salva modifiche.
8. Se si stanno modificando più record, ripetere le fasi da 5 a 7.

Eliminazione di record

La procedura seguente spiega come eliminare record utilizzando la console Route 53.
Per informazioni su come eliminare i record utilizzando l'API Route 53, consulta ChangeResourceRecordSetsAmazon Route 53 API Reference.

> **Note**
>
> Le modifiche ai registri richiedono tempo per propagarsi ai server DNS di Route 53. Attualmente, l'unico modo per verificare che le modifiche si siano propagate è utilizzare l'azione GetChangeAPI. In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Come eliminare record

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nella pagina Hosted Zones (Zone ospitate), scegliere la riga per la zona ospitata che contiene i record da eliminare.
3. Nell'elenco dei record, seleziona il record che desideri eliminare.

Per selezionare più record consecutivi, selezionare la prima riga, tenere premuto il tasto MAIUSC e selezionare l'ultima riga. Per selezionare più record non consecutivi, selezionare la prima riga, tenere premuto il tasto Ctrl e selezionare righe aggiuntive.

Non è possibile eliminare i record con un valore di NS o SOA per Type (Tipo).

4. Scegli Elimina.
5. Scegli Elimina per chiudere la finestra di dialogo.

Elencazione di record

La procedura seguente spiega come usare la console Amazon Route 53 per elencare i record in una zona ospitata. Per informazioni su come elencare i record utilizzando l'API Route 53, consulta ListResourceRecordSetsAmazon Route 53 API Reference.

Come elencare record

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Nella pagina Hosted zones (Zone ospitate) , scegli il nome di una zona ospitata.
4. Per modificare la modalità di ricerca, scegli l'icona a forma di ingranaggio in alto a destra della tabella Record. Scegli una delle seguenti opzioni:

   - Automatica

     In questa modalità, il servizio utilizza un filtro basato su una serie di record. Completa per meno di 2.000 record e veloce per più di 2.000 record.

   - Completa

     In questa modalità, tutti i filtri di ricerca sono disponibili, ma le prestazioni di ricerca potrebbero essere più lente.

   - Veloce

     In questa modalità, alcune funzionalità avanzate non sono disponibili, ma le prestazioni di ricerca saranno più veloci.

Per visualizzare solo i record selezionati, immetti i criteri di ricerca applicabili sopra l'elenco dei record. Nella modalità automatica, il comportamento di ricerca varia a seconda che la zona ospitata zone contenga fino a 2.000 record o più di 2.000 record:

Fino a 2.000 record e modalità completa

- Per visualizzare i record che hanno valori specifici, immetti un valore nella barra di ricerca e premi Invio. Ad esempio, per visualizzare i record che hanno un indirizzo IP che inizia con 192.0, digita il valore nel campo di ricerca e premi Invio.
- Per visualizzare solo i record con lo stesso tipo di record DNS, seleziona Tipo di record dall'elenco a discesa, quindi specifica il tipo di record.
- Per visualizzare solo record alias, seleziona Alias nell'elenco a discesa e specifica **`Yes`**.
- Per visualizzare solo record ponderati, seleziona Policy di routing nell'elenco a discesa e specifica **`WEIGHTED`**.

Più di 2.000 record e modalità veloce

- È possibile eseguire la ricerca solo su nomi di record, non sui valori dei record. Inoltre, non è possibile filtrare in base al tipo di record o sui record alias o ponderati.

  A tale scopo, posiziona il cursore nella casella di testo Filtro, seleziona Proprietà, quindi Nome record.
- Per i record che hanno tre etichette (tre parti separate da punti), quando specifichi un valore nel campo di ricerca e premi Invio, la console Route 53 esegue automaticamente una ricerca jolly nella terza etichetta da destra nel nome del record. Ad esempio, supponiamo che la zona ospitata, ad esempio esempio.com contenga 100 record denominati record1.esempio.com tramite record100.esempio.com. (Record1 è la terza etichetta da destra.) Ecco cosa succede quando si ricercano i seguenti valori:
  - record1 - La console Route 53 cerca record1*.esempio.com, che restituisce record1.esempio.com, record10.esempio.com tramite record19.esempio.com e record100.esempio.com.
  - record1.esempio.com: come nell'esempio precedente, la console cerca record1*.example.com e restituisce lo stesso record.
  - 1: la console ricerca 1*.example.com e non restituisce alcun record.
  - example: la console cerca example*.example.com e non restituisce alcun record.
  - esempio.com: in questo esempio, la console non esegue una ricerca con caratteri jolly. Si restituiscono tutti i record nella zona ospitata.

- Modalità di ricerca automatica: quando utilizzi questa modalità di ricerca, per poter effettuare la ricerca è necessario prima fornire una proprietà, ad esempio il nome del record.

> **Note**
>
> Se la terza etichetta da destra contiene uno o più trattini (ad esempio `third-label.example.com`) e si cerca la parte della terza etichetta immediatamente prima del trattino (`third` in questo esempio), Route 53 non restituirà alcun record. Al contrario, includere il trattino (cercare `third-`) o omettere il carattere immediatamente prima del trattino (cercare `third`).

- Per i record che hanno quattro o più etichette, è necessario specificare il nome esatto del record. Non sono supportate ricerche con caratteri jolly.. Ad esempio, se le zone ospitate includono un record denominato label4.record1.esempio.com, è possibile individuare quel record solo se si specifica label4.record1.esempio.com nel campo di ricerca.

Configurazione della firma DNSSEC in Amazon Route 53

La firma DNSSEC (Domain Name System Security Extensions) consente ai resolver DNS di verificare che una risposta DNS proviene da Amazon Route 53 e non è stata manomessa. Quando si utilizza la firma DNSSEC, ogni risposta per una zona ospitata viene firmata utilizzando la crittografia a chiave pubblica. Per una panoramica di DNSSEC, consulta la sezione DNSSEC di AWS re:Invent 2021 - Amazon Route 53: A year in review.

In questo capitolo, spieghiamo come abilitare la firma DNSSEC per Route 53, come utilizzare le chiavi di firma dei tasti () e come risolvere i problemi. KSKs Puoi lavorare con DNSSEC accedendo o programmaticamente con l'API. AWS Management Console Per ulteriori informazioni sull'utilizzo della CLI o sull'utilizzo SDKs di Route 53, vedere. Configura Amazon Route 53

Prima di abilitare la firma DNSSEC, tieni presente quanto segue:

- Per evitare interruzioni di una zona e che il dominio diventi indisponibile, è necessario risolvere rapidamente gli errori DNSSEC. Ti consigliamo vivamente di impostare un CloudWatch allarme che ti avvisi ogni volta che viene rilevato un `DNSSECKeySigningKeysNeedingAction` errore `DNSSECInternalFailure` or. Per ulteriori informazioni, consulta Monitoraggio delle zone ospitate tramite Amazon CloudWatch.

- Esistono due tipi di chiavi in DNSSEC: una chiave di firma delle chiavi (KSK) e una chiave di firma della zona (ZSK). Nella firma DNSSEC di Route 53, ogni KSK è basata su una chiave asimmetrica gestita dal cliente nella AWS KMS di tua proprietà. Sei responsabile della gestione KSK, che include la rotazione se necessario. La gestione ZSK viene eseguita da Route 53.
- Quando abiliti la firma DNSSEC per una zona ospitata, Route 53 limita la durata (TTL, Time to Live) a una settimana. Se si imposta un TTL di più di una settimana per i record nella zona ospitata, non viene visualizzato alcun errore. Tuttavia, Route 53 applica un TTL di una settimana per i record. I record con un TTL inferiore a una settimana e i record in altre zone ospitate che non dispongono della firma DNSSEC abilitata non sono interessati.
- Quando utilizzi la firma DNSSEC, le configurazioni multivendor non sono supportate. Se hai configurato dei server dei nomi white-label (noti anche come server dei nomi vanity o server dei nomi privati), assicurati che siano forniti da un unico provider DNS.
- Alcuni provider DNS non supportano i record Delegation Signer (DS) nei loro DNS autorevoli. Se la tua zona principale è ospitata da un provider DNS che non supporta le query DS (senza impostare un flag AA nella risposta alla query DS), quando abiliti DNSSEC nella relativa zona figlio, la zona figlio non potrà essere risolta. Assicurati che il tuo provider DNS supporti i record DS.
- Può essere utile impostare le autorizzazioni IAM per consentire a un altro utente, oltre al proprietario della zona, di aggiungere o rimuovere record nella zona. Ad esempio, il proprietario di una zona può aggiungere una KSK e abilitare la firma e potrebbe anche essere responsabile della rotazione delle chiavi. Tuttavia, qualcun altro potrebbe essere responsabile dell'utilizzo di altri record per la zona ospitata. Per un esempio di policy IAM, consultare Autorizzazioni di esempio per il proprietario di un record di dominio.
- Per verificare se il TLD supporta DNSSEC, consulta. Domini che è possibile registrare con Amazon Route 53

Argomenti

Abilitazione della firma DNSSEC e creazione di una catena di attendibilità

I passaggi incrementali si applicano al proprietario della zona ospitata e al manutentore della zona padre. Questa può essere la stessa persona, ma qualora non fosse cos', il proprietario della zona dovrebbe notificare e lavorare con il manutentore della zona padre.

Ti suggeriamo di seguire i passaggi di questo articolo per far firmare e includere la tua zona nella catena di fiducia. I seguenti passaggi ridurranno al minimo il rischio di onboarding su DNSSEC.

> **Note**
>
> Assicurati di leggere i prerequisiti prima di iniziare in Configurazione della firma DNSSEC in Amazon Route 53.

Per abilitare la firma DNSSEC, è necessario seguire tre fasi, come descritto nelle sezioni seguenti.

Argomenti

Fase 1: preparazione per l'abilitazione della firma DNSSEC

Le fasi di preparazione consentono di ridurre al minimo il rischio di onboarding su DNSSEC monitorando la disponibilità della zona e riducendo i tempi di attesa tra l'abilitazione della firma e l'inserimento del registro Delegation Signer (DS).

Per preparare l'abilitazione della firma DNSSEC

1. Monitora la disponibilità della zona.

   È possibile monitorare la zona per verificare la disponibilità dei nomi di dominio. Questo può aiutarti a risolvere eventuali problemi che potrebbero giustificare un ripristino dello stato precedente dopo aver abilitato la firma DNSSEC. È possibile monitorare i nomi di dominio con la maggior parte del traffico utilizzando la registrazione delle query. Per ulteriori informazioni su come impostare la registrazione delle query, consulta Monitoraggio di Amazon Route 53.

Il monitoraggio può essere effettuato tramite uno script di shell o un servizio di terze parti. Tuttavia, non dovrebbe essere l'unico segnale per determinare se sia necessario un ripristino dello stato precedente. Inoltre, potresti ricevere feedback dai tuoi clienti a causa della mancata disponibilità di un dominio.

2. Abbassa il TTL massimo della zona.

   Il TTL massimo della zona è il registro TTL più lungo della zona. Nella seguente zona di esempio, il TTL massimo della zona è 1 giorno (86.400 secondi).

Nome	TTL	Classe registro	Tipo di record	Dati registro
esempio.com.	900	IN	SOA	ns1.esempio.com. hostmaster.esempio.com. 2002022401 10800 15 604800 300
esempio.com.	900	IN	NS	ns1.esempio.com.
route53.esempio.com.	86400	IN	TXT	**some txt record**

   L'abbassamento del TTL massimo della zona contribuirà a ridurre il tempo di attesa tra l'abilitazione della firma e l'inserimento del registro Delegation Signer (DS). Ti suggeriamo di abbassare il TTL massimo della zona a 1 ora (3.600 secondi). Ciò permette di eseguire il ripristino allo stato precedente dopo appena un'ora, se un resolver ha problemi con la memorizzazione nella cache dei registri firmati.

   Ripristino dello stato precedente: annulla le modifiche TTL.

3. Abbassa il campo minimo SOA TTL e SOA.

Il campo minimo SOA è l'ultimo campo nei dati del registro SOA. Nel seguente registro SOA di esempio, il campo minimo ha il valore di 5 minuti (300 secondi).

Nome	TTL	Classe registro	Tipo di record	Dati registro
esempio.com.	900	IN	SOA	ns1.esempio.com. hostmaster.esempio.com. 2002022401 10800 15 604800 300

Il campo minimo SOA TTL e SOA determina per quanto tempo i resolver ricordano le risposte negative. Dopo aver abilitato la firma, i server dei nomi Route 53 iniziano a restituire i registri NSEC per le risposte negative. L'NSEC contiene informazioni che i resolver potrebbero utilizzare per sintetizzare una risposta negativa. Se è necessario eseguire il ripristino dello stato precedente a causa di informazioni NSEC che hanno causato l'assunzione di una risposta negativa per un nome da parte di un resolver, è sufficiente attendere il massimo del campo SOA TTL e il campo minimo SOA affinché il resolver interrompa l'assunzione.

Ripristino dello stato precedente: annulla le modifiche SOA.

4. Assicurati che le modifiche ai campi minimi TTL e SOA siano efficaci.

   Utilizzalo GetChangeper assicurarti che le modifiche apportate finora siano state propagate a tutti i server DNS di Route 53.

Fase 2: abilitazione della firma DNSSEC e creazione di una KSK

È possibile abilitare la firma DNSSEC e creare una chiave di firma delle chiavi (KSK) utilizzando AWS CLI o sulla console Route 53.

- CLI
- Console

Quando fornisci o crei una chiave KMS gestita dal cliente, esistono diversi requisiti da rispettare. Per ulteriori informazioni, consulta Utilizzo delle chiavi gestite dal cliente per DNSSEC.

CLI

Puoi usare una chiave già esistente, oppure crearne una eseguendo un comando AWS CLI come il seguente usando i propri valori per `hostedzone_id`, `cmk_arn`, `ksk_name`, e `unique_string` (per rendere unica la richiesta):

```
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
```

Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta Utilizzo delle chiavi gestite dal cliente per DNSSEC. Consulta anche CreateKeySigningKey.

Per abilitare la firma DNSSEC, esegui un AWS CLI comando come il seguente, utilizzando il tuo valore per: `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

Per ulteriori informazioni, vedere enable-hosted-zone-dnssece EnableHostedZone DNSSEC.

Console

Come abilitare la firma DNSSEC e creare una KSK

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata per la quale desideri abilitare la firma DNSSEC.
3. Nella scheda Firma DNSSEC, scegli Abilita firma DNSSEC.

> **Note**
>
> Se l'opzione in questa sezione è Disabilita firma DNSSEC, allora la fase iniziale dell'abilitazione della firma DNSSEC è già stata completata. Assicurati di stabilire,

o che esista già, una catena di attendibilità per la zona ospitata per DNSSEC. Per ulteriori informazioni, consulta Fase 3: come stabilire una catena di attendibilità.

4. Nella sezione Key-signing key (KSK) creation (Creazione di chiave di firma chiave (KSK)), scegli Create new KSK (Crea una nuova KSK), e sotto Provide KSK name Fornisci il nome KSK), inserisci un nome per il KSK che Route 53 creerà per te. I nomi possono contenere solo lettere, numeri e caratteri di sottolineatura (_). Deve essere univoco.
5. In CMK gestita dal cliente, scegli la chiave gestita dal cliente per Route 53 da utilizzare quando crea la KSK. È possibile utilizzare una chiave gestita dal cliente esistente che si applica alla firma DNSSEC oppure creare una nuova chiave gestita dal cliente.

   Quando fornisci o crei una chiave gestita dal cliente, esistono diversi requisiti da rispettare. Per ulteriori informazioni, consulta Utilizzo delle chiavi gestite dal cliente per DNSSEC.
6. Specifica l'alias per una chiave gestita dal cliente esistente. Se desideri utilizzare una nuova chiave gestita dal cliente, inserisci un alias per la chiave gestita dal cliente e Route 53 ne creerà una automaticamente.

   > **Note**
   >
   > Se scegli di fare in modo che Route 53 crei una chiave gestita dal cliente, tieni presente che si applicano addebiti separati per ogni chiave gestita dal cliente. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.
7. Scegli Abilita firma DNSSEC.

Dopo aver abilitato la firma della zona, completa i seguenti passagi: (che tu utilizzi la console o la CLI):

1. Assicurati che la firma della zona sia efficace.

   Se lo hai utilizzato AWS CLI, puoi utilizzare l'ID dell'operazione dall'output della `EnableHostedZoneDNSSEC()` chiamata per eseguire get-change o GetChangeper assicurarti che tutti i server DNS di Route 53 firmino le risposte (status =). `INSYNC`
2. Attendi almeno il TTL massimo della zona precedente.

Attendi che i resolver svuotino tutti i registri non firmati dalla cache. Per raggiungere questo obiettivo è necessario attendere almeno il TTL massimo della zona precedente. Nella zona `example.com` sopra, il tempo di attesa sarebbe di 1 giorno.

3. Monitoraggio della presenza di segnalazioni di problemi dei clienti.

   Dopo aver abilitato la firma della zona, i clienti potrebbero iniziare a vedere dei problemi relativi ai dispositivi di rete e ai resolver. Il periodo di monitoraggio suggerito è di 2 settimane.

   Di seguito sono riportati esempi dei problemi che potresti incontrare:

   - Alcuni dispositivi di rete potrebbero limitare le dimensioni della risposta DNS a meno di 512 byte, il che è troppo poco per alcune risposte firmate. Questi dispositivi di rete devono essere riconfigurati per permettere dimensioni di risposta DNS più grandi.
   - Alcuni dispositivi di rete eseguono un'ispezione approfondita sulle risposte DNS e ne eliminano alcuni registri che non capisce, come quelli usati per DNSSEC. Questi dispositivi devono essere riconfigurati.
   - Alcuni resolver di clienti attestano di poter accettare una risposta UDP più ampia, rispetto a quella supportata dalla rete. È possibile testare le funzionalità di rete e configurare i resolver in modo appropriato. Per ulteriori informazioni, consulta Server di test delle dimensioni delle risposte DNS.

Rollback: chiama DisableHostedZoneDNSSEC, quindi ripristina i passaggi. Fase 1: preparazione per l'abilitazione della firma DNSSEC

Fase 3: come stabilire una catena di attendibilità

Dopo aver abilitato la firma DNSSEC per una zona ospitata in Route 53, stabilisci una catena di attendibilità per la zona ospitata per completare la configurazione della firma DNSSEC. A tale scopo è possibile creare un record Delegation Signer (DS) nella zona ospitata padre, per la zona ospitata, utilizzando le informazioni fornite da Route 53. A seconda della posizione in cui il dominio è registrato, aggiungi il record alla zona ospitata padre in Route 53 o in un altro registrar di dominio.

Come stabilire una catena di attendibilità per la firma DNSSEC

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata per la quale stabilire una catena di attendibilità di DNSSEC. È necessario abilitare prima la firma DNSSEC.

3. Nella scheda Firma DNSSEC, in Firma DNSSEC, scegli Visualizza informazioni per creare record DS.

> **Note**
>
> Se l'opzione Visualizza le informazioni per creare un record DS non viene visualizzata in questa sezione, prima di stabilire la catena di attendibilità è necessario abilitare la firma DNSSEC. Scegli Enable DNSSEC signing (Abilita firma DNSSEC) e completa le fasi come descritte in Fase 2: abilitazione della firma DNSSEC e creazione di una KSK, quindi torna a queste fasi per stabilire la catena di attendibilità.

4. In Stabilisci una catena di attendibilità, scegli Registrar Route 53 o Un altro registrar di dominio, a seconda di dove è registrato il tuo dominio.
5. Usa i valori forniti dalla fase 3 per creare un registro DS per la zona ospitata padre in Route 53. Se il tuo dominio non è ospitato su Route 53, utilizza i valori forniti per creare un registro DS sul sito Web del registrar di domini.

   Stabilisci una catena di fiducia per la zona principale:

   - Se il tuo dominio è gestito tramite Route 53, procedi nel seguente modo:

     Assicurati di configurare l'algoritmo di firma (ECDSAP256SHA256 e tipo 13) e l'algoritmo digest (SHA-256 e tipo 2) corretti.

     Se Route 53 è il tuo registrar, procedi come segue nella console Route 53:

     1. Prendi nota dei valori di Tipo di chiave,Algoritmo di firma e Chiave pubblica. Nel riquadro di navigazione seleziona Registered domains (Domini registrati).
     2. Seleziona un dominio, quindi, accanto a Stato DNSSEC, scegli Gestisci chiavi.
     3. Nella finestra di dialogo Manage DNSSEC keys (Gestisci le chiavi DNSSEC), scegli l'opzione appropriata di Key type (Tipo di chiave) e Algorithm (Algoritmo) per Route 53 registrar (Registrar Route 53) dai menu a discesa.
     4. Copia la chiave pubblica per il registrar Route 53. Nella finestra di dialogo Manage DNSSEC keys (Gestisci chiavi DNSSEC), incolla il valore nella casella Public key (Chiave pubblica).
     5. Scegli Aggiungi.

Route 53 aggiungerà il record DS alla zona padre dalla chiave pubblica. Ad esempio, se il dominio è `example.com`, il record DS viene aggiunto alla zona DNS .com.

- Se il tuo dominio è gestito su un altro registro, segui le istruzioni nella sezione Un altro registrar di domini.

  Per assicurarti che i passaggi seguenti procedano senza intoppi, introduci un DS TTL basso nella zona padre. Qualora sia necessario ripristinare lo stato precedente delle modifiche, per un ripristino più rapido, noi suggeriamo di impostare DS TTL su 5 minuti (300 secondi).

  - Stabilisci una catena di fiducia per la zona riservata ai minori:

    Se la tua zona padre è amministrata da un altro registro, contatta il registrar per introdurre il registro DS per la tua zona. In genere non è possibile regolare il TTL del registro DS.

  - Se la tua zona padre è ospitata su Route 53, contatta il proprietario della zona padre per introdurre il registro DS per la tua zona.

    Fornisci il `$ds_record_value` al proprietario della zona padre. Puoi ottenerla facendo clic su Visualizza informazioni per creare il record DS nella console e copiando il campo del record DS, oppure chiamando l'API GetDNSsec e recuperando il valore del campo ": DSRecord

    ```
    aws --region us-east-1 route53 get-dnssec
                --hosted-zone-id $hostedzone_id
    ```

    Il proprietario della zona padre può inserire il registro cord tramite la console Route 53 o la CLI.

    - Per inserire il record DS utilizzando AWS CLI, il proprietario della zona principale crea e nomina un file JSON simile all'esempio seguente. Il proprietario della zona padre potrebbe nominare il file in modo simile a questo: `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"
                        }
                    ]
                }
            }
        ]
    }
}
```

Quindi, esegui il comando riportato di seguito:

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- Per inserire il registro cord DS utilizzando la console,

  Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

  Nel pannello di navigazione, scegli Hosted zones (Zone ospitate), il nome della tua zona ospitata e quindi cliccare il pulsante Create record (Crea registro). In Routing policy (Policy di routing), assicurati di scegliere il routing semplice.

  Nel campo Record name (Nome registro), immetti lo stesso nome di `$zone_name`, seleziona DS dal menu a discesa Record type (Tipo di registro) e inserisci il valore di `$ds_record_value` nel campo Value (Valore), e scegli Create records (Crea registri).

Ripristino dello stato precedente: rimuovi il DS dalla zona padre, attendi il DS TTL e quindi esegui il ripristino dello stato precedente dei passaggi per stabilire l'attendibilità. Se la zona padre è ospitata su Route 53, il proprietario della zona padre può modificare l'`Action` da `UPSERT` a`DELETE` nel file JSON ed esegui nuovamente l'interfaccia CLI di esempio sopra.

6. Attendi la propagazione degli aggiornamenti in base al TTL per i record di dominio.

   Se la zona principale si trova sul servizio DNS Route 53, il proprietario della zona principale può confermare la propagazione completa tramite l'GetChangeAPI.

In caso contrario, è possibile sondare periodicamente la zona padre per verificare la presenza del registro DS, quindi attendere altri 10 minuti dopo per aumentare la probabilità che l'inserimento del registro DS venga completamente propagato. Si noti che alcuni registrar hanno pianificato l'inserimento di DS, ad esempio una volta al giorno.

Quando si introduce il registro Delegation Signer (DS) nella zona padre, i resolver convalidati che hanno raccolto il DS inizieranno a convalidare le risposte dalla zona.

Per assicurarti che i passaggi per stabilire l'attendibilità procedano senza intoppi, completa quanto segue:

1. Trova il massimo NS TTL.

   Sono disponibili 2 set di registri NS associati alle zone:

   - Registro NS delegation: questo è il registro NS per la tua zona detenuto dalla zona padre. Puoi trovarlo eseguendo i seguenti comandi Unix (se la tua zona è example.com, la zona padre è com):

     ```
     dig -t NS com
     ```

     Seleziona uno dei registri NS e quindi esegui quanto segue:

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     Ad esempio:

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - Il registro NS nella zona: questo è il registro NS nella tua zona. Per aggiungerlo, puoi eseguire il comando Unix seguente:

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     Ad esempio:

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

     Nota il TTL massimo per entrambe le zone.

2. Attendi il massimo NS TTL.

Prima dell'inserimento del DS, i resolver ricevono una risposta firmata, ma non convalidano la firma. Quando il registro DS viene inserito, i resolver non lo vedono fino alla scadenza del registri NS per la zona. Quando i resolver recupererà nuovamente il registro NS, verrà restituito anche il registro DS.

Se il cliente sta eseguendo un resolver su un host con un clock non sincronizzato, assicurati che quest'ultimo sia entro 1 ora dall'ora corretta.

Dopo aver completato questo passaggio, tutti i resolver compatibili con DNSSEC convalideranno la tua zona.

3. Osserva la risoluzione dei nomi.

   Dovresti osservare che non ci sono problemi con i resolver che convalidano la tua zona. Assicurati di tenere conto anche del tempo necessario ai tuoi clienti per segnalarti i problemi.

   Noi suggeriamo di monitorare fino a 2 settimane.

4. (Facoltativo) Allunga DS e NS. TTLs

   Se sei soddisfatto della configurazione, puoi salvare le modifiche apportate a TTL e SOA. Nota che Route 53 limita il TTL a 1 settimana, per le zone firmate. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

   Se è possibile modificare il DS TTL, suggeriamo di impostarlo su 1 ora.

Disabilitazione della firma DNSSEC

I passaggi per disabilitare l'accesso DNSSEC nella Route 53 variano a seconda della catena di attendibilità di cui fa parte la zona ospitata.

Ad esempio, la zona ospitata potrebbe avere una zona padre con un record Delegation Signer (DS) come parte di una catena di attendibilità. La zona ospitata potrebbe anche essere essa stessa una zona padre per le zone figlio che hanno abilitato la firma DNSSEC, che è un'altra parte della catena di attendibilità. Esamina e determina l'intera catena di attendibilità per la zona ospitata prima di eseguire la procedura per disattivare la firma DNSSEC.

La catena di attendibilità per la zona ospitata che abilita la firma DNSSEC deve essere annullata con attenzione quando si disabilita la firma. Per rimuovere la zona ospitata dalla catena di attendibilità,

rimuovi tutti i record DS esistenti per la catena di attendibilità che include questa zona ospitata. Ciò significa che è necessario completare le operazioni seguenti nell'ordine:

1. Rimuovi tutti i record DS presenti in questa zona ospitata per le zone figlio che fanno parte di una catena di attendibilità.
2. Rimuovi il registro DS della zona padre. Se disponi di un'isola di attendibilità (dove non ci sono registri DS nella zona padre e nessun registro DS per le zone figlio), puoi ignorare questo passaggio.
3. Se non riesci a rimuovere i record DS, per rimuovere la zona dalla catena di attendibilità, rimuovi i record NS dalla zona padre. Per ulteriori informazioni, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

I seguenti passaggi incrementali ti permettono di monitorare l'efficacia dei singoli passaggi per evitare problemi di disponibilità DNS nella tua zona.

Come disabilitare la firma DNSSEC

1. Monitora la disponibilità della zona.

   È possibile monitorare la zona per verificare la disponibilità dei nomi di dominio. Questo può aiutarti a risolvere eventuali problemi che potrebbero giustificare un ripristino dello stato precedente dopo aver abilitato la firma DNSSEC. È possibile monitorare i nomi di dominio con la maggior parte del traffico utilizzando la registrazione delle query. Per ulteriori informazioni su come impostare la registrazione delle query, consulta Monitoraggio di Amazon Route 53.

   Il monitoraggio può essere effettuato tramite uno script di shell o tramite un servizio a pagamento. Tuttavia, non dovrebbe essere l'unico segnale per determinare se sia necessario un ripristino dello stato precedente. Inoltre, potresti ricevere feedback dai tuoi clienti a causa della mancata disponibilità di un dominio.
2. Trova l'attuale DS TTL.

   Puoi trovare il DS TTL eseguendo il seguente comando Unix:

   ```
   dig -t DS example.com example.com
   ```
3. Trova il massimo NS TTL.

   Sono disponibili 2 set di registri NS associati alle zone:

- Registro NS delegation: questo è il registro NS per la tua zona detenuto dalla zona padre. Puoi modificare questo comportamento eseguendo il seguente comando Unix:

  Per prima cosa trova il NS della tua zona padre (se la tua zona è example.com, la zona padre è com):

  ```
  dig -t NS com
  ```

  Seleziona uno dei registri NS e quindi esegui quanto segue:

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  Ad esempio:

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- Il registro NS nella zona: questo è il registro NS nella tua zona. Per aggiungerlo, puoi eseguire il comando Unix seguente:

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  Ad esempio:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  Nota il TTL massimo per entrambe le zone.

4. Rimuovi il registro DS della zona padre.

   Contatta il proprietario della zona padre per rimuovere il registro DS.

   Ripristino dello stato precedente: reinserisci il record DS, conferma che l'inserimento DS è efficace e attendi l'NS TTL massimo (non DS) prima che tutti i resolver ricomincino a convalidare.

5. Conferma che la rimozione del DS è efficace.

   Se la zona principale si trova sul servizio DNS Route 53, il proprietario della zona principale può confermare la propagazione completa tramite l'API. GetChange

   In caso contrario, è possibile sondare periodicamente la zona padre per verificare la presenza del registro DS, quindi attendere altri 10 minuti per aumentare la probabilità che la rimozione del registro DS venga completamente propagata. Nota che alcuni registrar hanno pianificato la rimozione del DS, ad esempio una volta al giorno.

6. Aspetta il DS TTL.

   Attendere che tutti i resolver non siano scaduti il registro DS dalle loro cache.

7. Disabilita la firma DNSSEC e disattiva la chiave di firma chiave (KSK) .

   - CLI
   - Console

   CLI

   Chiama DisableHostedZoneDNSSEC e. DeactivateKeySigningKey APIs

   Per esempio:

   ```
   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

   Come disabilitare la firma DNSSEC

   1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
   2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata per la quale desideri disabilitare la firma DNSSEC.
   3. Nella scheda Firma DNSSEC, scegli Disabilita firma DNSSEC.
   4. Nella pagina Disabilita firma DNSSEC seleziona una delle seguenti opzioni, a seconda dello scenario per la zona per cui disattivi la firma DNSSEC.
      - Solo zona padre: questa zona ha una zona padre con un record DS. In questo scenario, è necessario rimuovere il record DS della zona padre.
      - Solo zone figlio: questa zona ha un record DS per una catena di attendibilità con una o più zone figlio. In questo scenario, è necessario rimuovere il record DS della zona.

- Zone padre e figlio: questa zona ha sia un record DS per una catena di attendibilità con una o più zone figlio e una zona padre con un record DS. Per questo scenario, completa le operazioni seguenti nell'ordine riportato:

  a. Rimuovi i record DS della zona.

  b. Rimuovi i record DS della zona padre.

  Se possiedi un'isola di fiducia, puoi ignorare questa fase.

5. Determina il TTL per ogni registro DS che rimuovi nella fase 4 e, prima di continuare, assicurati che il periodo TTL più lungo sia scaduto.
6. Seleziona la casella di controllo per confermare di aver seguito i passi nell'ordine.
7. Digita disable nel campo, come riportato, quindi scegli Disabilita.

Come disattivare la chiave di firma chiave (KSK)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione scegli Hosted zones (Zone ospitate) e seleziona una zona ospitata per la quale desideri disabilitare la firma DNSSEC.
3. Nella sezione Chiavi di firma con chiave (KSKs), scegli il KSK che desideri disattivare e, in Azioni, scegli Modifica KSK, imposta lo stato KSK su Inattivo, quindi scegli Salva KSK.

ActivateKeySigningKeyEnableHostedZoneRollback: chiamata e DNSSEC. APIs

Per esempio:

```
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. Conferma che la disattivazione della firma della zona è efficace.

Usa l'ID della `EnableHostedZoneDNSSEC()` chiamata da eseguire GetChangeper assicurarti che tutti i server DNS di Route 53 abbiano smesso di firmare le risposte (status =). `INSYNC`

9. Osserva la risoluzione dei nomi.

   Dovresti osservare che non ci sono problemi che causano i resolver da convalidare la tua zona. Attendi 1-2 settimane, per tenere conto anche del tempo necessario ai tuoi clienti per segnalarti i problemi.

10. (Facoltativo) Pulizia.

    Se non riattiverai la firma, puoi ripulire il processo DeleteKeySigningKeyed eliminare KSKs la corrispondente chiave gestita dal cliente per risparmiare sui costi.

Utilizzo delle chiavi gestite dal cliente per DNSSEC

Quando abiliti l'accesso DNSSEC in Amazon Route 53, Route 53 crea una chiave per l'identificazione delle chiavi (KSK) per tuo conto. Per creare un KSK, Route 53 deve utilizzare una chiave gestita dal cliente AWS Key Management Service che supporti DNSSEC. In questa sezione vengono descritti i dettagli e i requisiti per la chiave gestita dal cliente che sono utili quando si lavora con il protocollo DNSSEC.

Quando utilizzi chiavi gestite dal cliente per DNSSEC, tieni presente quanto segue:

- La chiave gestita dal cliente utilizzata con la firma DNSSEC deve trovarsi nella regione Stati Uniti orientali (Virginia settentrionale).
- La chiave gestita dal cliente deve essere una chiave asimmetrica gestita dal cliente con una specifica della chiave ECC_NIST_P256. Queste chiavi gestite dal cliente vengono utilizzate solo per la firma e la verifica. Per informazioni sulla creazione di una chiave gestita dal cliente asimmetrica, consulta Creazione di chiavi gestite dal cliente asimmetriche nella Guida per gli sviluppatori. AWS Key Management Service Per informazioni su come trovare la configurazione crittografica di una chiave gestita dal cliente esistente, consulta Visualizzazione della configurazione crittografica delle chiavi gestite dal cliente nella Guida per gli sviluppatori. AWS Key Management Service
- Se crei personalmente una chiave gestita dal cliente da utilizzare con DNSSEC in Route 53, è necessario includere le istruzioni di policy specifiche della chiave che concedano a Route 53 le autorizzazioni richieste. Perché possa creare una KSK per tuo conto, Route 53 deve poter

accedere alla chiave gestita dal cliente. Per ulteriori informazioni, consulta Autorizzazioni delle chiavi gestite dal cliente di Route 53 richieste per la firma DNSSEC.

- Route 53 può creare una chiave gestita dal cliente AWS KMS da utilizzare con la firma DNSSEC senza autorizzazioni aggiuntive. AWS KMS Tuttavia, se desideri modificare la chiave dopo la sua creazione è necessario disporre di autorizzazioni specifiche. Le autorizzazioni specifiche che è necessario avere sono: `kms:UpdateKeyDescription`, `kms:UpdateAlias` e `kms:PutKeyPolicy`.
- Tieni presente che si applicano addebiti separati per ogni chiave gestita dal cliente di cui disponi, indipendentemente dal fatto che tu crei la chiave gestita dal cliente o che Route 53 la crei per te. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.

Utilizzo delle chiavi per la firma dei tasti () KSKs

Quando abiliti la firma DNSSEC, Route 53 crea una chiave per la firma delle chiavi (KSK) per tuo conto. Puoi averne fino a due KSKs per zona ospitata in Route 53. Dopo aver abilitato la firma DNSSEC, puoi aggiungere, rimuovere o modificare il tuo. KSKs

Tieni presente quanto segue quando lavori con: KSKs

- Prima di poter eliminare una KSK, è necessario modificare la KSK per impostarne lo stato su Inattivo.
- Quando la firma DNSSEC è abilitata per una zona ospitata, Route 53 limita il TTL a una settimana. Se imposti un TTL per i record nella zona ospitata su più di una settimana, non viene visualizzato un errore ma Route 53 applica un TTL di una settimana.
- Per evitare interruzioni di una zona e che il dominio diventi indisponibile, è necessario risolvere rapidamente gli errori DNSSEC. Ti consigliamo vivamente di impostare un CloudWatch allarme che ti avvisi ogni volta che viene rilevato un `DNSSECKeySigningKeysNeedingAction` errore `DNSSECInternalFailure` or. Per ulteriori informazioni, consulta Monitoraggio delle zone ospitate tramite Amazon CloudWatch.
- Le operazioni KSK descritte in questa sezione consentono di ruotare le zone. KSKs Per ulteriori informazioni e un step-by-step esempio, consulta DNSSEC Key Rotation nel post del blog Configurazione della firma e della convalida DNSSEC con Amazon Route 53.

Per utilizzare in AWS Management Console, segui le indicazioni riportate KSKs nelle sezioni seguenti.

Aggiunta di una chiave di firma delle chiavi (KSK)

Quando abiliti la firma DNSSEC, Route 53 crea una chiave per la firma delle chiavi (KSK) per tuo conto. È possibile aggiungere anche KSKs separatamente. Puoi averne fino a due KSKs per zona ospitata in Route 53.

Quando crei una KSK, devi fornire (o richiedere a Route 53 di creare) una chiave gestita dal cliente da utilizzare con la KSK. Quando fornisci o crei una chiave gestita dal cliente, esistono diversi requisiti da rispettare. Per ulteriori informazioni, consulta Utilizzo delle chiavi gestite dal cliente per DNSSEC.

Completa queste fasi per aggiungere una KSK nella AWS Management Console.

Come aggiungere una KSK

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata.
3. Nella scheda Firma DNSSEC, in Chiavi di firma a chiave (KSKs), scegli Passa alla visualizzazione avanzata, quindi, in Azioni, scegli Aggiungi KSK.
4. In KSK, inserisci un nome per la KSK che Route 53 creerà per te. I nomi possono contenere solo lettere, numeri e caratteri di sottolineatura (_). Deve essere univoco.
5. Immetti l'alias per una chiave gestita dal cliente che si applica alla firma DNSSEC oppure immetti un alias per una nuova chiave gestita dal cliente gestita dal cliente che Route 53 creerà automaticamente.

   > **Note**
   >
   > Se scegli di fare in modo che Route 53 crei una chiave gestita dal cliente, tieni presente che si applicano addebiti separati per ogni chiave gestita dal cliente. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.

6. Scegli Crea KSK.

Modifica di una chiave di firma delle chiavi (KSK)

È possibile modificare lo stato di una KSK in modo che sia Attiva o Inattiva. Quando una KSK è attiva, Route 53 la utilizza per la firma DNSSEC. Prima di poter eliminare una KSK, è necessario modificare la KSK per impostarne lo stato su Inattivo.

Completa queste fasi per aggiungere una KSK nella AWS Management Console.

Come modificare una KSK

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata.
3. Nella scheda Firma DNSSEC, in Chiavi di firma a chiave (KSKs), scegli Passa alla visualizzazione avanzata, quindi, in Azioni, scegli Modifica KSK.
4. Apporta gli aggiornamenti desiderati alla KSK, quindi scegli Salva.

Eliminazione di una chiave di firma delle chiavi (KSK)

Prima di poter eliminare una KSK, è necessario modificare la KSK per impostarne lo stato su Inattivo.

Uno dei motivi per cui potresti eliminare un KSK è come parte della rotazione delle chiavi di routine. Una best practice consiste nel ruotare periodicamente le chiavi di crittografia. È possibile che l'organizzazione disponga di indicazioni standard per quanto spesso ruotare le chiavi.

Completa queste fasi per eliminare una KSK nella AWS Management Console.

Come eliminare una KSK

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione scegli Zone ospitate e seleziona una zona ospitata.
3. Nella scheda Firma DNSSEC, in Chiavi di firma a chiave (KSKs), scegli Passa alla visualizzazione avanzata, quindi in Azioni, scegli Elimina KSK.
4. Segui le istruzioni per confermare l'eliminazione della KSK.

Chiave KMS e gestione ZSK in Route 53

Questa sezione descrive la pratica corrente utilizzata da Route 53 per le zone abilitate per la firma DNSSEC.

> **Note**
>
> Route 53 utilizza la seguente regola, che potrebbe essere modificata. Qualsiasi modifica futura non ridurrà la posizione di sicurezza della tua zona o di Route 53.

In che modo Route 53 utilizza il codice associato al tuo KSK AWS KMS

In DNSSEC, la KSK viene utilizzata per generare la firma del registro della risorsa (RRSIG) per il set di registri della risorsa DNSKEY. Tutti `ACTIVE` KSKs sono utilizzati nella generazione RRSIG. Route 53 genera un RRSIG chiamando l'`Sign` AWS KMS API sulla chiave KMS associata. Per ulteriori informazioni, consulta la sezione Firma nella Guida di riferimento dell'API AWS KMS . Questi RRSIGs non vengono conteggiati ai fini del limite stabilito per il record di risorse della zona.

Il RRSIG ha una scadenza. Per RRSIGs evitare che scadano, RRSIGs vengono rinfrescati regolarmente rigenerandoli ogni uno-sette giorni.

RRSIGs Vengono inoltre aggiornati ogni volta che si chiama uno di questi: APIs

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Ogni volta che Route 53 esegue un aggiornamento, ne generiamo 15 RRSIGs per coprire i prossimi giorni nel caso in cui la chiave KMS associata diventi inaccessibile. Per stimare il costo delle chiavi KMS, è possibile presumere un aggiornamento regolare una volta al giorno. Una chiave KMS potrebbe diventare inaccessibile in seguito a modifiche involontarie alla policy della chiave KMS. Una chiave KMS inaccessibile imposta lo stato della KSK associata su `ACTION_NEEDED`. Ti consigliamo vivamente di monitorare questa condizione impostando un CloudWatch allarme ogni volta che viene rilevato un `DNSSECKeySigningKeysNeedingAction`

errore, perché i resolver di convalida inizieranno a fallire le ricerche dopo la scadenza dell'ultimo RRSIG. Per ulteriori informazioni, consulta Monitoraggio delle zone ospitate tramite Amazon CloudWatch.

Modalità di gestione della ZSK della zona da parte di Route 53

Ogni nuova zona ospitata con firma DNSSEC abilitata avrà una chiave di firma zona (ZSK) `ACTIVE`. La ZSK viene generata separatamente per ogni zona ospitata ed è di proprietà di Route 53. L'algoritmo chiave corrente è. ECDSAP256 SHA256

Inizieremo a eseguire regolarmente la rotazione ZSK sulla zona entro 7-30 giorni dall'inizio della firma. Attualmente, Route 53 utilizza il metodo di sostituzione periodica delle chiavi previa pubblicazione. Per ulteriori informazioni, consulta la sezione Sostituzione periodica delle chiavi previa pubblicazione. Questo metodo introduce un'altra ZSK nella zona. La rotazione viene ripetuta ogni 7-30 giorni.

Route 53 sospenderà la rotazione ZSK se uno dei KSK della zona è in `ACTION_NEEDED` stato, perché Route 53 non sarà in grado di rigenerare i set di record di risorse RRSIGs per DNSKEY per tenere conto delle modifiche nello ZSK della zona. La rotazione ZSK riprende automaticamente dopo che la condizione è stata risolta.

Prove DNSSEC dell'inesistenza in Route 53

> **Note**
>
> Route 53 utilizza la seguente regola, che potrebbe essere modificata. Qualsiasi modifica futura non ridurrà la posizione di sicurezza della tua zona o di Route 53.

In DNSSEC sono disponibili tre tipi di prova dell'inesistenza:

- Prova dell'inesistenza di un registro corrispondente al nome della query.
- Prova dell'inesistenza di un registro corrispondente al tipo di query.
- Prova dell'esistenza di un registro jolly utilizzato per generare il registro in risposta.

Route 53 implementa la prova dell'inesistenza di un registro corrispondente al nome della query utilizzando il metodo BL. Per ulteriori informazioni, consulta la sezione BL. È un metodo che produce una rappresentazione compatta della prova e impedisce l'ingresso nella zona.

Nei casi in cui esiste un record che corrisponde al nome della query ma non al tipo di query (ad esempio, l'interrogazione per web.example). com/AAAA but there is only web.example.com/ Apresent), restituiamo un record NSEC (next secure) minimo contenente tutti i tipi di record di risorse supportati.

Quando Route 53 sintetizza una risposta da un registro con caratteri jolly, la risposta non sarà accompagnata da un successivo registro sicuro, o record NSEC per il carattere jolly. Tale registro NSEC viene utilizzato in alcune implementazioni, in genere quelle che eseguono la firma non in linea, per impedire che le firme dei registri della risorsa (RRSIG) nella risposta vengano riutilizzate per falsificare una risposta diversa. Route 53 utilizza la firma online per i record non DNSKey per generare una risposta RRSIGs specifica che non può essere riutilizzata per una risposta diversa.

Risoluzione dei problemi relativi alla firma DNSSEC

Le informazioni contenute in questa sezione possono aiutarti a risolvere i problemi relativi alla firma DNSSEC, tra cui l'attivazione, la disabilitazione e l'utilizzo delle chiavi di firma delle chiavi (). KSKs

Abilitazione di DNSSEC

Prima di iniziare ad abilitare la firma DNSSEC, assicurati di aver letto i prerequisiti riportati in Configurazione della firma DNSSEC in Amazon Route 53.

Disabilitazione di DNSSEC

Per disabilitare in modo sicuro il DNSSEC, Route 53 verificherà se la zona di destinazione si trova nella catena di attendibilità. Verifica se l'elemento padre della zona di destinazione ha dei record NS e dei record DS della zona di destinazione. Se la zona di destinazione non è risolvibile pubblicamente, ad esempio se riceve una risposta SERVFAIL durante l'interrogazione di NS e DS, Route 53 non sarà in grado di determinare se è sicuro disabilitare DNSSEC. Puoi contattare la tua zona principale per risolvere questi problemi e riprovare a disabilitare il DNSSEC in un secondo momento.

Lo stato della KSK è Operazione necessaria

Un KSK può cambiare il suo stato in Azione necessaria (o `ACTION_NEEDED` in uno KeySigningKeystato) quando Route 53 DNSSEC perde l'accesso a un server corrispondente AWS KMS key (a causa di una modifica delle autorizzazioni o dell'eliminazione). AWS KMS key

Se lo stato di una KSK è Action needed (Azione richiesta), significa che alla fine causerà un'interruzione della zona per i client che utilizzano i resolver di convalida DNSSEC e tu dovrai agire rapidamente per evitare che una zona di produzione diventi irrisolvibile.

Per risolvere il problema, assicurati che la chiave gestita dal cliente su cui si basa la tua KSK sia abilitata e abbia le corrette autorizzazioni. Per ulteriori informazioni sulle autorizzazioni richieste, consulta Autorizzazioni delle chiavi gestite dal cliente di Route 53 richieste per la firma DNSSEC.

Dopo aver corretto il KSK, attivalo nuovamente utilizzando la console o il AWS CLI, come descritto in. Fase 2: abilitazione della firma DNSSEC e creazione di una KSK

Per evitare che questo problema si verifichi in futuro, prendi in considerazione l'aggiunta di una Amazon CloudWatch metrica per tracciare lo stato del KSK, come suggerito in. Configurazione della firma DNSSEC in Amazon Route 53

Lo stato della KSK è Errore interno

Quando un KSK presenta lo stato di errore interno (o `INTERNAL_FAILURE` in uno KeySigningKeystato), non è possibile lavorare con nessun'altra entità DNSSEC finché il problema non viene risolto. È necessario intervenire prima di poter utilizzare la firma DNSSEC, incluso l'utilizzo di questa KSK o di un'altra KSK.

Per risolvere il problema, prova nuovamente ad attivare o disattivare la KSK.

Per risolvere il problema quando lavori con APIs, prova ad abilitare la firma (EnableHostedZoneDNSSEC) o disabilitare la firma (DNSSEC). DisableHostedZone

È importante correggere i problemi Errore internoquanto prima. Non è possibile apportare altre modifiche alla zona ospitata fino a quando non si corregge il problema, ad eccezione delle operazioni per risolvere Errore interno.

Utilizzo AWS Cloud Map per creare record e controlli sanitari

Se si desidera instradare il traffico Internet o il traffico all'interno di un Amazon VPC a componenti dell'applicazione o di microservizi, puoi utilizzare AWS Cloud Map per creare automaticamente i record e, facoltativamente, i controlli dell'integrità. Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Cloud Map.

Comportamenti e limitazioni di DNS

La messaggistica DNS è soggetta a fattori che influiscono su come si creano e utilizzano zone ospitate e record. Questa sezione descrive questi fattori.

Dimensioni massime della risposta

Per la conformità agli standard DNS, le dimensioni delle risposte inviate su UDP non superano i 512 byte. Le risposte che superano 512 byte vengono troncate e il resolver deve emettere di nuovo la richiesta su TCP. Se il resolver supporta EDNS0 (secondo quanto definito nella specifica RFC 2671) e pubblicizza l'opzione di EDNS0 ad Amazon Route 53, Route 53 consente risposte fino a 4.096 byte su UDP, senza troncamento.

Elaborazione della sezione autorevole

Per query dall'esito positivo, Route 53 collega record di server di nomi (NS) per le zone ospitate alla sezione Authority della risposta DNS. Per i nomi che non vengono trovati (risposte NXDOMAIN), Route 53 collega il record origine di autorità (SOA) (secondo quanto definito nella specifica RFC 1035) per la zona ospitata pertinente alla sezione Authority della risposta DNS.

Elaborazione di sezioni aggiuntive

Route 53 collega record alla sezione aggiuntiva. Se i record sono noti e appropriati, il servizio collega record A o AAAA per qualsiasi target di un record MX, CNAME, NS o SRV citato nella sezione delle risposte. Per ulteriori informazioni su questi tipi di record DNS, consulta Tipi di record DNS supportati.

Utilizzo di Traffic Flow per instradare il traffico DNS

Traffic Flow semplifica enormemente il processo di creazione e gestione dei record in configurazioni ampie e complesse.

La gestione dei record correlati in una zona ospitata può essere difficile nelle seguenti circostanze:

- Si dispone di molte risorse che eseguono la stessa operazione, ad esempio server Web che servono il traffico per lo stesso dominio.
- Si desidera creare una struttura complessa di record utilizzando record alias e una combinazione di policy di routing di Route 53, ad esempio latenza, failover e ponderata.

Vantaggi del flusso di traffico

Per semplificare il monitoraggio dei record e delle relative relazioni, Traffic Flow semplifica la creazione di record DNS con le seguenti funzionalità:

Visual editor (Editor visivo)

L'editor visivo Traffic Flow consente di creare alberi di record complessi e di visualizzare le relazioni tra i record. Ad esempio, potrebbe essere necessario creare una configurazione in cui i record alias di latenza fanno riferimento ai record ponderati e i record ponderati fanno riferimento alle risorse in più Regioni AWS. Ogni configurazione è nota come policy di traffico. Puoi creare tutte le policy di traffico che desideri senza alcun costo.

Controllo delle versioni

Puoi creare più versioni di una policy di traffico in modo da non dover ricominciare da capo quando la configurazione cambia. Le versioni precedenti continuano ad esistere fino a quando non vengono eliminate; esiste un limite predefinito di 1000 versioni per policy di traffico. Facoltativamente, puoi fornire una descrizione per ciascuna versione.

Creazione e aggiornamento automatico dei record

Una policy di traffico può rappresentare dozzine o addirittura centinaia di record. Traffic Flow consente di creare automaticamente tutti questi record creando un record relativo alla politica del traffico. Specificare la zona ospitata e il nome del record a livello della radice della struttura, ad esempio example.com o www.example.com; tutti gli altri record nella struttura verranno

creati automaticamente da Route 53. Il record root, ovvero il record della policy di traffico, viene visualizzato nella lista dei record per la tua zona ospitata; tutti gli altri record sono nascosti.

Quando crei una nuova versione di una policy di traffico, puoi aggiornare in modo selettivo i record delle policy di traffico creati utilizzando la versione precedente della policy di traffico. Quando aggiorni un record delle policy di traffico, tutti gli altri record nella struttura vengono aggiornati automaticamente da Route 53. Inoltre, puoi ripristinare rapidamente le modifiche aggiornando nuovamente un record delle policy di traffico per utilizzare una versione precedente di una policy di traffico.

> **Note**
>
> Puoi utilizzare Traffic Flow per creare record solo in zone pubbliche ospitate.

Policy di routing della geoprossimità

Quando usi Traffic Flow, puoi capire in modo più intuitivo come il traffico viene indirizzato a ciascuno dei tuoi endpoint globali utilizzando la mappa di geoprossimità sulla tela visiva di Traffic Flow. Per ulteriori informazioni, consulta Routing di geoprossimità.

Riutilizzo di più record in zone ospitate differenti

Puoi utilizzare una policy di traffico per creare automaticamente record in più zone ospitate pubbliche. Ad esempio, se stai utilizzando gli stessi server Web per più nomi di dominio, puoi utilizzare la stessa policy di traffico per creare record delle policy di traffico nelle zone ospitate per example.com, example.org ed example.net.

Quando un client invia una query per il nome del record radice, ad esempio example.com o www.example.com, Route 53 risponde alla query in base alla configurazione della policy di traffico utilizzata per creare il record delle policy di traffico corrispondente.

Per ogni record delle policy di traffico viene addebitato un costo mensile. Per ulteriori informazioni, consulta la sezione "Traffic Flow" in Prezzi di Amazon Route 53.

Per ridurre al minimo questi costi, è possibile creare uno o più record alias in una zona ospitata che fanno riferimento a un record delle policy di traffico in tale zona ospitata. Ad esempio, puoi creare un record delle policy di traffico per example.com e quindi creare un record alias per www.example.com che faccia riferimento al record delle policy di traffico.

Creazione e gestione delle policy di traffico

Argomenti

Creazione di una policy di traffico

Per creare una policy di traffico, esegui la procedura seguente.

Per creare una policy di traffico

1. Progetta la tua configurazione. Per ulteriori informazioni su come funzionano le configurazioni di routing DNS complesse, consulta Configurazione di un failover DNS Creazione di controlli sanitari su Amazon Route 53 .
2. In base alla progettazione della tua configurazione, crea i controlli dell'integrità che desideri utilizzare per i tuoi endpoint.
3. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
4. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
5. Selezionare Create traffic policy (Crea policy di traffico).
6. Nella pagina Name policy (Rinomina policy), specificare i valori applicabili. Per ulteriori informazioni, consulta I valori che specifichi durante la creazione di una policy di traffico.
7. Scegli Next (Successivo).
8. Nella pagina Create traffic policy (Crea policy di traffico) nome policy v1, specificare i valori applicabili. Per ulteriori informazioni, consulta I valori che specifichi durante la creazione di una policy di traffico.

   Puoi eliminare regole, endpoint e rami di una policy di traffico nei seguenti modi:

- Per eliminare una regola o un endpoint, fare clic sulla x nell'angolo in alto a destra della casella.

  > **Important**
  >
  > Se elimini una regola che dispone di regole figlio ed endpoint, Amazon Route 53 elimina anche tutti i figli.

- Se colleghi due regole alla stessa regola figlio o allo stesso endpoint e desideri eliminare una delle connessioni, ferma il cursore sulla connessione che desideri eliminare e fai clic sulla x per tale connessione.

9. Selezionare Create traffic policy (Crea policy di traffico).
10. Facoltativo: nella pagina Create policy records with traffic policy (Crea record di policy con policy di traffico), utilizzare la nuova policy di traffico per creare uno o più record di policy in una zona ospitata. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento di un record di policy. Puoi anche creare record di policy in un secondo momento, sia nella stessa zona ospitatache in altre zone ospitate.

    Se non desideri creare subito i record delle politiche, scegli Ignora questo passaggio e la console visualizzerà l'elenco delle politiche sul traffico e dei record delle politiche che hai creato utilizzando l' AWS account corrente.
11. Se hai specificato le impostazioni per i record di policy nella fase precedente, scegli Create policy record (Crea record di policy).

I valori che specifichi durante la creazione di una policy di traffico

Quando crei una policy di traffico devi specificare i seguenti valori.

-
-
-
-
-
-
-

Nome policy

Inserisci un nome che descrive la policy di traffico. Tale valore viene visualizzato nell'elenco delle policy di traffico nella console. Non puoi modificare il nome di una policy di traffico dopo averla creata.

Versione

Tale valore viene assegnato automaticamente da Amazon Route 53 quando crei una policy di traffico o una nuova versione di una policy esistente.

Version description (Descrizione versione)

Inserisci una descrizione che si applica a questa versione della policy di traffico. Tale valore viene visualizzato nell'elenco delle versioni di policy di traffico nella console.

DNS type (Tipo DNS)

Scegli il tipo di DNS che desideri che Amazon Route 53 assegni a tutti i record quando crei un record di policy utilizzando questa versione di policy di traffico. Per un elenco di tipo supportati, consulta Tipi di record DNS supportati.

> **Important**
>
> Se crei una nuova versione di una policy di traffico esistente, puoi modificare il tipo di DNS. Tuttavia, non puoi modificare un record di policy e scegliere una versione di policy di traffico che dispone di un tipo di DNS diverso dalla versione di policy di traffico utilizzata per creare il record di policy. Ad esempio, se hai creato un record di policy utilizzando una versione di policy di traffico che ha come DNS Type (Tipo DNS) A, non puoi modificare i record di policy e scegliere una versione di policy di traffico che abbia qualsiasi altro valore per DNS Type (Tipo DNS).

Se desideri indirizzare il traffico verso le seguenti AWS risorse, scegli il valore applicabile:

- CloudFront distribuzione: scegli A: indirizzo IP in IPv4 formato o AAAA: indirizzo IP in IPv6 formato.
- ELB Application Load Balancer: scegliete A: indirizzo IP in IPv4 formato o AAAA: indirizzo IP in formato. IPv6
- Sistema di bilanciamento del carico ELB Classic: scegli A: indirizzo IP nel IPv4 formato o AAAA: indirizzo IP nel formato. IPv6

- Sistema di bilanciamento del carico di rete ELB: scegli A: indirizzo IP nel IPv4 formato o AAAA: indirizzo IP nel formato. IPv6
- Ambiente Elastic Beanstalk: scegli A: indirizzo IP nel formato. IPv4
- Bucket Amazon S3 configurato come endpoint del sito Web: scegli A: indirizzo IP in formato. IPv4

Connect to (Connettiti a)

Scegli la regola o l'endpoint applicabile in base alla progettazione per la tua configurazione.

Failover rule (Regola di failover)

Scegli questa opzione per configurare il failover attivo/passivo, in cui una risorsa prende tutto il traffico quando è disponibile e le altre risorse prendono tutto il traffico quando la prima risorsa non è disponibile.

Per ulteriori informazioni, consulta Failover attivo-passivo.

Regola di geolocalizzazione

Scegli questa opzione se desideri che Amazon Route 53 risponda alle query DNS in base alla posizione dei tuoi utenti.

Per ulteriori informazioni, consulta Routing di geolocalizzazione.

Quando selezioni Geolocation rule (Regola di geolocalizzazione), puoi anche scegliere il paese o lo stato negli Stati Uniti da cui provengono le richieste.

Latency rule (Regola di latenza)

Scegli questa opzione quando disponi di risorse in più data EC2 center Amazon che svolgono la stessa funzione e desideri che Route 53 risponda alle query DNS con le risorse che offrono la latenza migliore.

Quando scegli Regola di latenza puoi anche scegliere una Regione AWS.

Per ulteriori informazioni, consulta Routing basato sulla latenza.

Geoproximity rule (Regola di geoprossimità)

Scegli questa opzione se desideri che Route 53 risponda alle query DNS in base alla posizione delle risorse e, facoltativamente, in base a un bias specificato da te. Il bias consente di inviare più traffico verso una risorsa o più traffico lontano da una risorsa.

Quando scegli Geoproximity rule (Regola di geoprossimità), inserisci i seguenti valori:

Endpoint location (Posizione endpoint)

Scegli il valore applicabile:

- Personalizzato (inserisci le coordinate): se l'endpoint non è una AWS risorsa, scegli Personalizzato (inserisci le coordinate).
- R Regione AWS: Se l'endpoint è una AWS risorsa, scegli Regione AWS quello in cui hai creato la risorsa.
- Una zona AWS locale: se l'endpoint è una AWS risorsa, scegli la zona AWS locale in cui hai creato la risorsa.

Se utilizzi AWS Local Zones, devi prima abilitarle. Per ulteriori informazioni, consulta Nozioni di base sulle zone locali nella Guida per l'utente delle zone locali AWS .

Per le zone locali disponibili, consulta Posizioni delle zone locali AWS.

Per conoscere la differenza tra Regioni AWS e Local Zones, consulta Regions and Zones nella Amazon EC2 User Guide.

> **Important**
>
> Una singola politica di routing di geoprossimità non può contenere due o più località geograficamente situate all'interno della stessa area metropolitana.
> Inoltre, alcune Regioni AWS Local Zones, come US West (Oregon) e Portland, USA, sono situate troppo vicine l'una all'altra per essere utilizzate nell'ambito della stessa politica di routing di geoprossimità. Se hai bisogno di indirizzare il traffico verso più di una località all'interno della stessa area metropolitana, definisci invece una politica di routing di geoprossimità che si traduca in una regola di routing ponderato 50/50 (WRR) per due diversi endpoint nell'area, distribuendo così il traffico in modo uniforme tra tali endpoint.

Coordinates

Se hai selezionato Custom (enter coordinates) (Personalizzata (inserire le coordinate)) per Endpoint location (Posizione endpoint), inserisci la latitudine e la longitudine della posizione della risorsa. Tieni presente quanto segue:

- La latitudine rappresenta la posizione a sud (negativo) o a nord (positivo) dell'equatore. I valori validi sono compresi tra -90 e 90 gradi.
- La longitudine rappresenta la posizione a ovest (negativo) o a est (positivo) del meridiano primario. I valori validi sono compresi tra -180 e 180 gradi.
- Puoi ottenere latitudine e longitudine da alcune applicazioni di mappatura online. Ad esempio, in Google Maps, l'URL per una posizione specifica la latitudine e longitudine:

  https://www.google.com/maps/@ 47.6086111, - 122.3409953, 20z
- Puoi inserire fino a due decimali di precisione, ad esempio 47.63. Se specifichi un valore con maggiore precisione, Route 53 tronca il valore alle due cifre dopo il decimale. Per latitudine e longitudine all'equatore, 0,01 gradi corrisponde a circa 0,69 miglia.

Bias

Per modificare facoltativamente le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica il valore applicabile per Bias:

- Per espandere le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica un numero intero positivo tra 1 e 99 per il bias. Route 53 riduce le dimensioni delle regioni adiacenti.
- Per ridurre le dimensioni della regione geografica da cui Route 53 indirizza il traffico a una risorsa, specifica un numero negativo tra -1 e -99 per il bias. Route 53 espande le dimensioni delle regioni adiacenti.

> **Important**
>
> L'effetto della modifica del valore di Bias è relativo, basata sulla posizione di altre risorse, anziché assoluto, in base alla distanza. Di conseguenza, l'effetto di una modifica è difficile prevedere. Ad esempio, a seconda della posizione in cui si trovano le tue risorse, modificare il bias da 10 a 15 può fare la differenza tra l'aggiunta e la sottrazione di una notevole quantità di traffico dall'area metropolitana di New York. È consigliabile modificare il bias di piccoli incrementi, valutare i risultati e quindi apportare modifiche aggiuntive, se necessario.

Per ulteriori informazioni, consulta Routing di geoprossimità.

Multivalue answer rule (Regola di risposta multivalore)

Scegli questa opzione se desideri che Route 53 risponda alle query DNS con un massimo di otto risposte integre, selezionate approssimativamente a caso.

Per ulteriori informazioni, consulta Routing di risposta multivalore.

Weighted rule (Regola ponderata)

Seleziona questa opzione se disponi di più risorse che eseguono la stessa funzione (ad esempio, server Web utilizzati per lo stesso sito Web) e desideri che Route 53 instradi il traffico verso le risorse in proporzioni specificate (ad esempio, 1/3 a un server e 2/3 all'altro).

Quando selezioni Weighted rule (Regola ponderata), digita il peso che desideri applicare a questa regola.

Per ulteriori informazioni, consulta Routing ponderato.

Endpoint

Scegli questa opzione per specificare la risorsa, ad esempio una CloudFront distribuzione o un sistema di bilanciamento del carico Elastic Load Balancing, a cui desideri indirizzare le query DNS.

Existing rule (Regola esistente)

Seleziona questa opzione se desideri instradare le query DNS a una regola esistente in questa policy di traffico. Ad esempio, puoi creare due o più regole di geolocalizzazione in grado di instradare le query per diversi paesi alla stessa regola di failover. La regola di failover può quindi instradare le query a due sistemi di bilanciamento del carico Elastic Load Balancing.

Questa opzione non è disponibile se la policy di traffico non include alcuna regola.

Existing endpoint (Endpoint esistente)

Seleziona questa opzione se desideri instradare le query DNS a un endpoint esistente. Ad esempio, se disponi di due regole di failover, puoi instradare le query DNS per entrambe le opzioni (secondarie) Su failover allo stesso sistema di bilanciamento del carico Elastic Load Balancing.

Questa opzione non è disponibile se la policy di traffico non include alcun endpoint.

Value type (Tipo di valore)

Scegli l'opzione applicabile:

CloudFront distribuzione

Scegliete questa opzione se desiderate indirizzare il traffico verso una CloudFront distribuzione. L'opzione è disponibile solo se hai scelto A: indirizzo IP in IPv4 formato per tipo DNS o AAAA: indirizzo IP in IPv6 formato per tipo DNS.

Application Load Balancer ELB

Seleziona questa opzione se desideri instradare il traffico a un Application Load Balancer Elastic Load Balancing. L'opzione è disponibile solo se hai scelto A: indirizzo IP in IPv4 formato o AAAA: indirizzo IP in formato per il tipo IPv6 DNS.

Classic Load Balancer ELB

Seleziona questa opzione se desideri instradare il traffico a un Classic Load Balancer Elastic Load Balancing. L'opzione è disponibile solo se hai scelto A: indirizzo IP nel IPv4 formato o AAAA: indirizzo IP nel IPv6 formato per il tipo DNS.

Network Load Balancer ELB

Seleziona questa opzione se desideri instradare il traffico a un Network Load Balancer Elastic Load Balancing. L'opzione è disponibile solo se hai scelto A: indirizzo IP nel IPv4 formato o AAAA: indirizzo IP nel IPv6 formato per il tipo DNS.

Ambienti Elastic Beanstalk

Seleziona questa opzione se desideri indirizzare il traffico a un ambiente Elastic Beanstalk. L'opzione è disponibile solo se hai scelto A: indirizzo IP in IPv4 formato per il tipo DNS.

S3 website endpoint (Endpoint del sito Web S3)

Seleziona questa opzione se desideri instradare il traffico a un bucket Amazon S3 configurato come endpoint del sito Web. L'opzione è disponibile solo se hai scelto A: indirizzo IP in IPv4 formato per il tipo DNS.

Digita il valore DNS type (Tipo DNS)

Seleziona questa opzione se desideri che Route 53 risponda alle query DNS utilizzando il valore nel campo Valore. Ad esempio, se hai scelto A come valore per DNS type (Tipo DNS) quando

hai creato la policy di traffico, questa opzione nell'elenco Value type (Tipo di valore) sarà Type A value (Valore tipo A). Ciò richiede l'immissione di un indirizzo IP in IPv4 formato nel campo Valore. Route 53 risponderà alle query DNS che vengono instradate a questo endpoint con l'indirizzo IP nel campo Valore.

Valore

Scegli o digita un valore in base all'opzione che hai selezionato per Value type (Tipo di valore):

CloudFront distribuzione

Scegli una CloudFront distribuzione dall'elenco delle distribuzioni associate all' AWS account corrente.

Application Load Balancer ELB

Scegli un sistema di bilanciamento del carico dell'applicazione Elastic Load Balancing dall'elenco dei sistemi di bilanciamento del carico associati all'account corrente. AWS

Classic Load Balancer ELB

Scegli un sistema di bilanciamento del carico Elastic Load Balancing Classic dall'elenco dei sistemi di bilanciamento del carico associati all'account corrente. AWS

Network Load Balancer ELB

Scegli un sistema di bilanciamento del carico Elastic Load Balancing Network dall'elenco dei sistemi di bilanciamento del carico associati all'account corrente. AWS

Ambienti Elastic Beanstalk

Scegli un ambiente Elastic Beanstalk dall'elenco degli ambienti associati all'attuale Account AWS.

S3 website endpoint (Endpoint del sito Web S3)

Scegli un bucket Amazon S3 dall'elenco dei bucket Amazon S3 configurati come endpoint del sito Web e associati all'account corrente. AWS

> **Important**
>
> Quando crei un record di policy basato su questa policy di traffico, il bucket che scegli qui deve corrispondere al nome di dominio (ad esempio, www.esempio.com) specificato per

Policy record DNS name nel record di policy. Se Valore e Nome DNS record policy non corrispondono, Amazon S3 non risponderà alle query DNS per il nome di dominio.

Digita il valore DNS type (Tipo DNS)

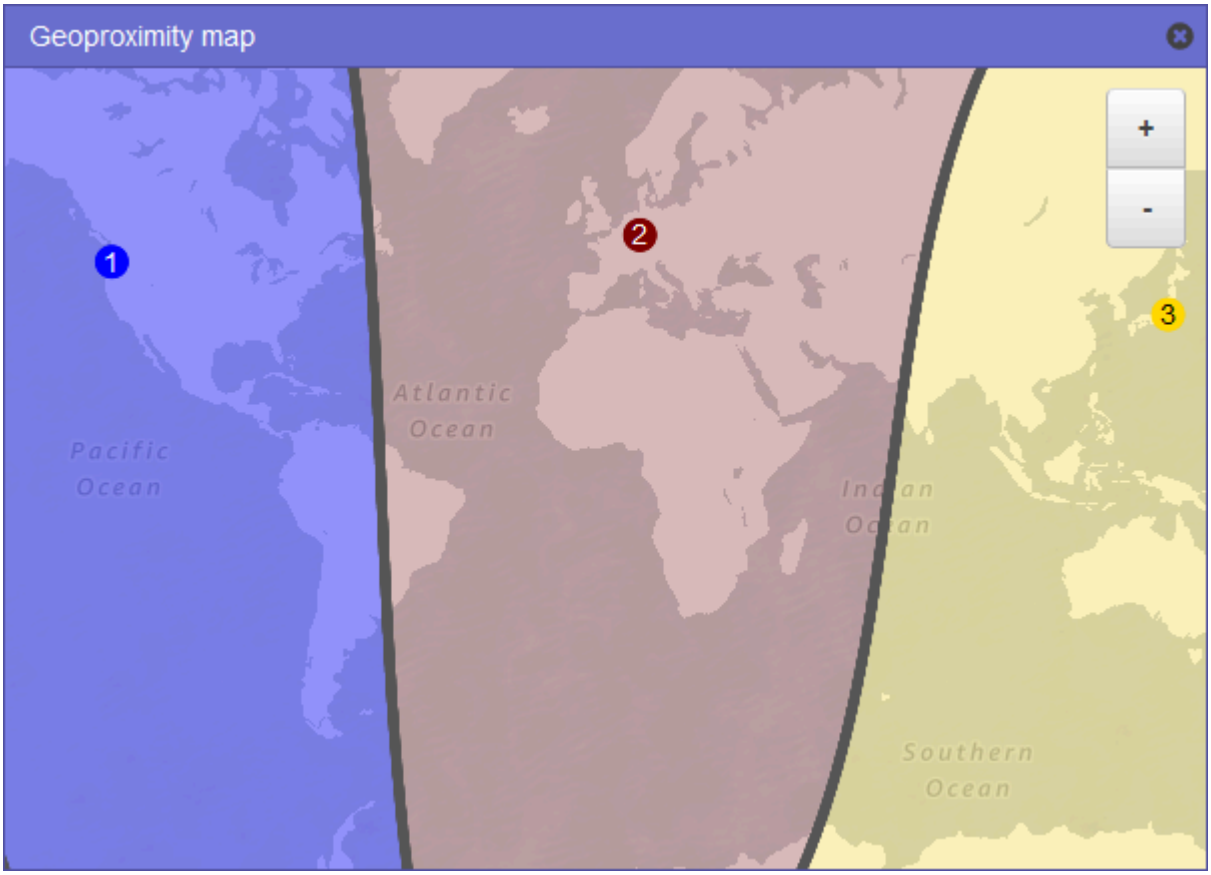
Inserisci un valore che corrisponda al valore specificato per il DNS type (Tipo DNS) quando hai avviato questa policy di traffico. Ad esempio, se hai selezionato MX per DNS type (Tipo DNS), digita due valori: la priorità che desideri assegnare a un server e-mail e il nome di dominio del server di posta, ad esempio `10 sydney.mail.example.com`.

Per ulteriori informazioni sui tipi di DNS supportati, consulta Tipi di record DNS supportati.

Visualizzazione di una mappa che mostra l'effetto delle impostazioni sulla geoprossimità

Una regola di geoprossimità consente di specificare le posizioni delle risorse, sia all'interno Regioni AWS che nelle Local Zones e, utilizzando latitudine e longitudine, in luoghi diversi.AWS Quando crei una regola di geoprossimità, per impostazione predefinita Route 53 instrada il traffico Internet alla risorsa più vicina ai propri utenti. Inoltre, puoi scegliere di instradare più o meno traffico a una risorsa specificando un bias che espande o restringe le dimensioni della regione geografica da cui il traffico viene instradato a una risorsa. Per ulteriori informazioni sul routing di geoprossimità, consulta Routing di geoprossimità.

È possibile visualizzare una cartina che mostra l'effetto delle tue attuali impostazioni di geoprossimità. Ad esempio, se disponi di risorse negli Stati Uniti occidentali (Oregon), Europa (Francoforte) e Asia Pacifico (Tokyo) e, se non specifichi un bias, la mappa appare simile alla seguente.



Per visualizzare la mappa per una regola di geoprossimità, scegliere l'icona del grafico accanto a Show geoproximity map (Mostra mappa di geoprossimità). (Nella parte superiore della regola viene visualizzata questa regola.) Per nascondere la mappa, scegliere di nuovo l'icona oppure scegliere la x nell'angolo in alto a destra della mappa.

Tieni presente quanto segue:

- La mappa ha una precisione di circa 16 chilometri.
- La mappa regola automaticamente quando aggiungi, modifichi o elimini le regioni oppure quando modifichi l'impostazione bias di una regione.
- Il numero di regione e il colore in ciascuna definizione di regola corrisponde ai numeri e ai colori sulla mappa.
- È possibile ingrandire e ridurre la finestra per visualizzare più o meno dettagli. Utilizza i pulsanti + e - sulla mappa, un touchpad oppure la rotellina del mouse per modificare il livello di zoom.
- È possibile spostare la mappa all'interno della finestra della mappa per visualizzare aree specifiche. Utilizza un touchpad o fai clic e trascina la mappa con un mouse. Inoltre, puoi spostare la finestra della mappa in una finestra del browser.

- Se si dispone di più di una regola di geoprossimità in una policy, è possibile visualizzare la mappa solo per una regola alla volta.

Creazione di versioni aggiuntive di una policy di traffico

Quando modifichi una policy di traffico, Amazon Route 53 crea automaticamente un'altra versione della policy di traffico e conserva le versioni precedenti a meno che non vi sia un'esplicita richiesta di rimozione da parte dell'utente. La nuova versione ha lo stesso nome della policy di traffico in fase di modifica, ma è distinta dalla versione originale da un numero di versione che Route 53 incrementa automaticamente. Puoi basare la nuova versione di una policy di traffico su qualsiasi versione esistente di una policy di traffico con lo stesso nome.

Route 53 non riutilizza i numeri di versione per nuove versioni di una determinata policy di traffico. Ad esempio, se si creano tre versioni di MyTrafficPolicy, si eliminano le ultime due versioni e quindi si crea un'altra versione, la nuova versione è la versione 4. Conservando le versioni precedenti, Route 53 garantisce che sia possibile eseguire il roll back a una configurazione precedente, nel caso in cui una nuova configurazione non instradi il traffico come previsto.

Per creare una nuova versione di policy di traffico, esegui la procedura seguente.

Per creare un'altra versione di una policy di traffico

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
3. Scegli il nome della policy di traffico per cui desideri creare una nuova versione.
4. Nella tabella Traffic policy versions (Versioni policy di traffico) nella parte superiore della pagina, seleziona la casella di controllo per la versione della policy di traffico che desideri utilizzare come base per la nuova versione di policy di traffico.
5. Seleziona Edit policy as new version (Modifica policy come nuova versione).
6. Nella pagina Update description (Aggiorna descrizione), digita una descrizione per la nuova versione di policy di traffico. È consigliabile specificare una descrizione che distingue questa versione dalle altre versioni della stessa policy di traffico. Quando crei un nuovo record di policy, il valore specificato viene visualizzato nella lista di versioni disponibili per questa policy di traffico.
7. Scegli Next (Successivo).

8. Aggiorna la configurazione come applicabile. Per ulteriori informazioni, consulta I valori che specifichi durante la creazione di una policy di traffico.

   Puoi eliminare regole, endpoint e rami di una policy di traffico nei seguenti modi:

   - Per eliminare una regola o un endpoint, fare clic sulla x nell'angolo in alto a destra della casella.

     > **Important**
     >
     > Se elimini una regola che dispone di regole figlio ed endpoint, Route 53 elimina anche tutti i figli.

   - Se colleghi due regole alla stessa regola figlio o allo stesso endpoint e desideri eliminare una delle connessioni, ferma il cursore sulla connessione che desideri eliminare e fai clic sulla x per tale connessione.

9. Una volta completata la modifica, seleziona Save as new version (Salva come nuova versione).
10. Facoltativo: specifica le impostazioni per creare uno o più record di policy in una zona ospitata utilizzando la nuova versione di policy di traffico. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento di un record di policy. Puoi anche creare record di policy in un secondo momento, sia nella stessa zona ospitatache in altre zone ospitate.

    Se non desideri creare subito i record delle politiche, scegli Ignora questo passaggio e la console visualizzerà l'elenco delle politiche sul traffico e dei record delle politiche che hai creato utilizzando l' AWS account corrente.
11. Se hai specificato le impostazioni per i record di policy nella fase precedente, scegli Create policy record (Crea record di policy).

Creazione di una policy di traffico mediante l'importazione di un documento in formato JSON

Puoi creare una nuova policy di traffico o una nuova versione di una policy di traffico esistente tramite l'importazione di un documento in formato JSON che descrive tutti gli endpoint e le regole che desideri includere nella policy di traffico. Per informazioni sul formato del documento JSON e diversi esempi che puoi copiare ed esaminare, consulta Formato del documento della policy di traffico nella Documentazione di riferimento delle API di Amazon Route 53.

Il modo più semplice per ottenere il documento in formato JSON per una versione esistente di policy sul traffico consiste nell'utilizzare il comando `get-traffic-policy` nella CLI. AWS Per ulteriori informazioni, consulta la sezione get-traffic-policy nella Documentazione di riferimento della AWS CLI .

Il file JSON creato dal comando `get-traffic-policy` include barre rovesciate (\) utilizzate come caratteri di escape. Prima di importare il file JSON, sostituisci tutte le barre rovesciate con caratteri null.

Per creare una policy di traffico mediante l'importazione di un documento JSON

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Per creare una nuova policy di traffico tramite l'importazione di un documento in formato JSON, esegui questa procedura:
   a. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
   b. Selezionare Create traffic policy (Crea policy di traffico).
   c. Nella pagina Name policy (Rinomina policy), specificare i valori applicabili. Per ulteriori informazioni, consulta I valori che specifichi durante la creazione di una policy di traffico.
   d. Passa alla fase 4.
3. Per creare una nuova versione di una policy di traffico esistente tramite l'importazione di un documento in formato JSON, esegui questa procedura:
   a. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
   b. Scegli il nome della policy di traffico su cui desideri basare la nuova versione.
   c. Nella tabella Traffic policy versions (Versioni policy di traffico), seleziona la casella di controllo per la versione su cui desideri basare la nuova versione.
   d. Seleziona Edit policy as new version (Modifica policy come nuova versione).
   e. Nella pagina Update description (Aggiorna descrizione), digitare una descrizione per la nuova versione.
   f. Passa alla fase 4.
4. Scegli Next (Successivo).
5. Seleziona Import traffic policy (Importa policy di traffico).
6. Digita una nuova policy di traffico, incolla un esempio di policy di traffico o incollare una policy di traffico esistente.

7. Seleziona Import traffic policy (Importa policy di traffico).

Visualizzazione di versioni di policy di traffico e dei record di policy associati

Puoi visualizzare tutte le versioni che hai creato per una policy di traffico, nonché tutti i record di policy creati utilizzando ciascuna delle versioni della policy di traffico.

Per visualizzare le versioni della policy di traffico e i record di policy associati

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
3. Scegli il nome di una policy di traffico.
4. Nella tabella superiore sono elencate tutte le versioni che hai creato di una policy di traffico. La tabella include le informazioni seguenti:

   Version number (Numero versione)

   Il numero di ciascuna versione di una policy di traffico che hai creato. Se scegli il numero di versione, la console visualizza la configurazione per tale versione.

   Number of policy records (Numero di record di policy)

   Il numero di record di policy creati utilizzando questa versione di policy di traffico.

   DNS type (Tipo DNS)

   Il tipo di DNS specificato durante la creazione della versione di policy di traffico.

   Version description (Descrizione versione)

   La descrizione che hai specificato durante la creazione della versione di policy di traffico.
5. Nella tabella inferiore sono elencati tutti i record di policy create utilizzando le versioni di policy di traffico nella tabella superiore. La tabella include le informazioni seguenti:

   Policy record DNS name (Nome DNS record policy)

   I nomi DNS ai quali hai associato la policy di traffico.

   Stato

   I valori possibili sono:

Applied (Applicato)

Route 53 ha terminato la creazione o l'aggiornamento di un record di policy e dei record corrispondenti.

Creazione

Route 53 sta creando i record per un nuovo record di policy.

Aggiornamento in corso

Hai aggiornato un record di policy e Route 53 sta creando un nuovo gruppo di record che sostituirà il gruppo di record esistente per il nome DNS specificato.

Eliminazione in corso

Route 53 sta eliminando un record di policy e i record associati.

Non riuscito

Route 53 non ha potuto creare o aggiornare il record di policy e i record associati.

Version used (Versione utilizzata)

Indica la versione della policy di traffico che hai utilizzato per creare il record di policy.

DNS type (Tipo DNS)

Il tipo di DNS di tutti i record che Route 53 ha creato per questo record di policy. Quando modifichi un record di policy, devi specificare una versione di policy di traffico che ha lo stesso tipo di DNS del tipo di DNS per il record di policy che stai modificando.

TTL (in seconds) (TTL (in secondi))

La quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore elevato (ad esempio, 172.800 secondi o due giorni), il costo del servizio di Route 53 risulta inferiore in quanto i resolver ricorsivi inviano le richieste a Route 53 con minore frequenza. Tuttavia, è necessario più tempo affinché abbiano effetto le modifiche ai record (ad esempio, un nuovo indirizzo IP) in quanto i resolver ricorsivi utilizzano per periodi più lunghi i valori nella loro cache anziché richiedere a Route 53 le informazioni più recenti.

Eliminazione di versioni di policy di traffico e policy di traffico

Per eliminare una policy di traffico, devi eliminare tutte le versioni (inclusa l'originale) che hai creato per la stessa. Inoltre, per eliminare una versione di policy di traffico, devi eliminare tutti i record di policy che hai creato utilizzando la versione della policy di traffico.

> **Important**
>
> Se elimini record di policy utilizzati da Amazon Route 53 per rispondere a query DNS, Route 53 smette di rispondere alle query per i nomi DNS corrispondenti. Ad esempio, se Route 53 utilizza il record di policy per www.esempio.com per rispondere alle query DNS per www.esempio.com ed elimini il record di policy, gli utenti non saranno in grado di accedere al tuo sito o applicazione Web usando il nome di dominio www.esempio.com.

Per eliminare le versioni di policy di traffico e, facoltativamente, una policy di traffico, esegui la procedura seguente:

Per eliminare versioni di policy di traffico e una policy di traffico

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
3. Scegli il nome della policy di traffico per cui desideri eliminare versioni di policy di traffico e che, facoltativamente, vuoi eliminare completamente.
4. Se le versioni di policy di traffico che desideri eliminare nella parte superiore della tabella appaiono nella colonna Version used (Versione utilizzata) nella tabella inferiore, seleziona le caselle di controllo per i record di policy corrispondenti nella tabella inferiore.

   Ad esempio, se desideri eliminare la versione 3 di una policy di traffico, ma hai creato uno dei record di policy nella tabella inferiore utilizzando la versione 3, seleziona la casella di controllo per quel record di policy.
5. Seleziona Delete policy records (Elimina record di policy).
6. Seleziona il pulsante di aggiornamento per la tabella inferiore per aggiornare la visualizzazione finché i record di policy eliminati non sono più visualizzati nella tabella.
7. Nella tabella superiore, seleziona le caselle di controllo per le versioni di policy di traffico che desideri eliminare.

8. Seleziona Delete version (Elimina versione).
9. Se hai eliminato tutte le versioni di policy di traffico nella fase precedente e desideri eliminare anche la policy di traffico, seleziona il pulsante di aggiornamento per la tabella superiore per aggiornare la visualizzazione fino a quando la tabella non sarà vuota.
10. Nel riquadro di navigazione, selezionare Traffic policies (Policy di traffico).
11. Nell'elenco di tutte le policy di traffico, seleziona la casella di controllo per la policy di traffico che desideri eliminare.
12. Seleziona Delete traffic policy (Elimina policy di traffico).

Creazione e gestione di record di policy

Per instradare il traffico Internet alle risorse specificate durante la creazione della policy di traffico, è necessario creare uno o più record di policy. Ogni record di policy identifica la zona ospitata in cui si desidera creare il record di policy e il nome di dominio o sottodominio verso cui si desidera instradare il traffico. Ad esempio, se si desidera instradare il traffico per www.esempio.com, è necessario specificare l'ID della zona ospitata per la zona ospitata esempio.com e si specifica www.esempio.com per il nome DNS del record della policy.

Se si desidera utilizzare la stessa policy di traffico per instradare il traffico per più di un nome di dominio o di sottodominio, sono disponibili due opzioni:

- È possibile creare un record di policy per ogni dominio o un nome di sottodominio.
- È possibile creare un record di policy e quindi creare CNAME o record alias che si riferiscono al record della policy.

Ad esempio, se si desidera utilizzare la stessa policy di traffico per esempio.com, example.net e example.org, è possibile eseguire una delle operazioni seguenti:

- Creare un record di policy per ognuno di essi.
- Creare un record di policy per uno di essi e quindi creare record CNAME nelle zone ospitate per gli altri due. Nei due record CNAME, è necessario specificare il nome del record per cui è stato creato un record di policy.

Se si desidera utilizzare la stessa policy di traffico per un dominio e i relativi sottodomini, ad esempio esempio.com e www.esempio.com, è possibile creare un record di policy per un nome e quindi creare

record alias per il resto. Ad esempio, è possibile creare un record di policy per esempio.com e quindi creare un record alias per www.esempio.com che abbia il record esempio.com come destinazione alias.

> **Note**
>
> Per ogni record di policy che crei, sarai soggetto a un addebito mensile. Se si desidera utilizzare la stessa policy di traffico per più nomi di dominio o sottodominio, è possibile utilizzare i record CNAME o alias per ridurre i costi di:
>
> - Se si crea un record di policy e uno o più record CNAME che si riferiscono al record della policy, si paga solo per il record di policy e per le query DNS per i record CNAME.
> - Se si crea un record di policy e uno o più record alias nella stessa zona ospitata che si riferiscono al record della policy, si paga solo per il record della policy e per le query DNS per i record alias.

Argomenti

Creazione di record di policy

Per creare un record di policy, esegui la procedura seguente.

> **Important**
>
> Per ogni record di policy che crei, sarai soggetto a un addebito mensile. Se successivamente elimini il record di policy, l'addebito sarà ripartito proporzionalmente. Per ulteriori informazioni, consulta la sezione "Flusso di traffico" in Prezzi di Amazon Route 53.

Per creare un record di policy

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Policy records (Record di policy).
3. Nella pagina Policy records (Record di policy), seleziona Create policy records (Crea record di policy).
4. Nella pagina Create policy records (Crea record di policy), specifica i valori applicabili. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento di un record di policy.
5. Seleziona Create policy records (Crea record di policy).

   Possono essere necessari alcuni minuti prima che lo stato del record di policy creato venga visualizzato come Applicato.
6. Se desideri creare record di policy in un'altra zona ospitata, ripeti le fasi da 3 a 5.

> **Note**
>
> Se lo stato del record di policy è Non riuscito, per ottenere maggiori informazioni sull'errore scegli il pulsante informazioni accanto allo stato. Se hai bisogno di ulteriore assistenza e desideri contattare l' AWS assistenza, vedi Come posso ottenere supporto tecnico da AWS?

Valori che specifichi durante la creazione o l'aggiornamento di un record di policy

Quando crei o aggiorni un record di policy, specifichi i valori seguenti

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

Policy di traffico

Scegli la policy di traffico la cui configurazione desideri utilizzare per il record di policy.

Version

Scegli la versione della policy di traffico la cui configurazione desideri utilizzare per il record di policy.

Se stai aggiornando un record di policy esistente, devi scegliere una versione per la quale il tipo di DNS corrisponde all'attuale tipo di DNS del record della policy. Ad esempio, se il tipo di DNS del record della policy è A, devi scegliere una versione per la quale il tipo di DNS è A.

Hosted zone

Scegli la zona ospitata in cui desideri creare una policy record utilizzando la policy di traffico e la versione specificata. Non puoi modificare il valore della Hosted zone (Zona ospitata) dopo la creazione di un record di policy.

Policy record DNS name (Nome DNS record policy)

Quando crei un record di policy, digita il nome di dominio o sottodominio per cui desideri che Route 53 risponda alle query DNS utilizzando la configurazione nella policy di traffico specificata e nella versione specificata.

Per utilizzare la stessa configurazione per più di un nome di dominio o di sottodominio nella zona ospitata, seleziona Add another policy record (Aggiungi un altro record di policy), quindi immetti il nome di dominio o di sottodominio applicabile e il TTL.

Non puoi modificare il valore di Policy record DNS name (Nome DNS record di policy) dopo la creazione di un record di policy.

TTL (in seconds) (TTL (in secondi))

Digita la quantità di tempo, in secondi, per cui desideri che i resolver ricorsivi DNS memorizzino nella cache le informazioni relative a questo record. Se specifichi un valore elevato (ad esempio, 172.800 secondi, o due giorni), il costo del servizio di Route 53 risulta inferiore in quanto i resolver ricorsivi inviano le richieste a Route 53 con minore frequenza. Tuttavia, è necessario più tempo affinché abbiano effetto le modifiche ai record (ad esempio, un nuovo indirizzo IP) in quanto i resolver ricorsivi utilizzano per periodi più lunghi i valori nella loro cache anziché richiedere a Route 53 le informazioni più recenti.

Aggiornamento di record di policy

Per aggiornare le impostazioni in un record di policy, esegui la procedura seguente.

Per aggiornare un record di policy

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Policy records (Record di policy).
3. Nella pagina Policy records (Record di policy), seleziona la casella di controllo per il record di policy che desideri aggiornare e seleziona Edit policy record (Modifica record di policy).
4. Nella pagina Edit policy record (Modifica record di policy), specifica i valori applicabili. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento di un record di policy.
5. Seleziona Edit policy record (Modifica record di policy).

   Possono essere necessari alcuni minuti prima che lo stato del record di policy creato venga visualizzato come Applicato.
6. Se desideri aggiornare un altro record di policy, ripeti le fasi da 3 a 5.

> **Note**
>
> Se lo stato del record di policy è Non riuscito, per ottenere maggiori informazioni sull'errore scegli il pulsante informazioni accanto allo stato. Se hai bisogno di ulteriore assistenza e desideri contattare l' AWS assistenza, vedi Come posso ottenere supporto tecnico da AWS?

Eliminazione di record di policy

Per eliminare record di policy, esegui la procedura seguente.

> **Important**
>
> Se elimini record di policy utilizzati da Amazon Route 53 per rispondere a query DNS, Route 53 smette di rispondere alle query per i nomi DNS corrispondenti. Ad esempio, se Route 53 utilizza il record di policy per www.esempio.com per rispondere alle query DNS per

www.esempio.com ed elimini il record di policy, gli utenti non saranno in grado di accedere al tuo sito o applicazione Web usando il nome di dominio www.esempio.com.

Per eliminare un record di policy

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione seleziona Policy records (Record di policy).
3. Nella pagina Policy records (Record di policy), seleziona le casella di controllo per i record di policy che desideri eliminare e seleziona Delete policy record (Elimina record di policy).

   Attendi alcuni minuti e aggiorna la pagina per assicurarti che il record di policy scompaia dall'elenco.

Che cos'è Amazon Route 53 Resolver?

Amazon Route 53 Resolver risponde in modo ricorsivo alle richieste DNS provenienti da AWS risorse per record pubblici, nomi DNS specifici di Amazon VPC e zone private ospitate di Amazon Route 53 ed è disponibile per impostazione predefinita in tutti. VPCs

> **Note**
>
> Amazon Route 53 Resolver in precedenza era chiamato server Amazon DNS, ma è stato rinominato quando sono state introdotte le regole Resolver e gli endpoint in entrata e in uscita. Per ulteriori informazioni, consulta Server DNS Amazon nella Guida per l'utente di Amazon Virtual Private Cloud.

Un Amazon VPC si connette a un Route 53 Resolver su un indirizzo IP VPC+2. Questo indirizzo VPC +2 si connette a Route 53 Resolver all'interno di una zona di disponibilità.

Un Route 53 Resolver risponde automaticamente alle query DNS per:

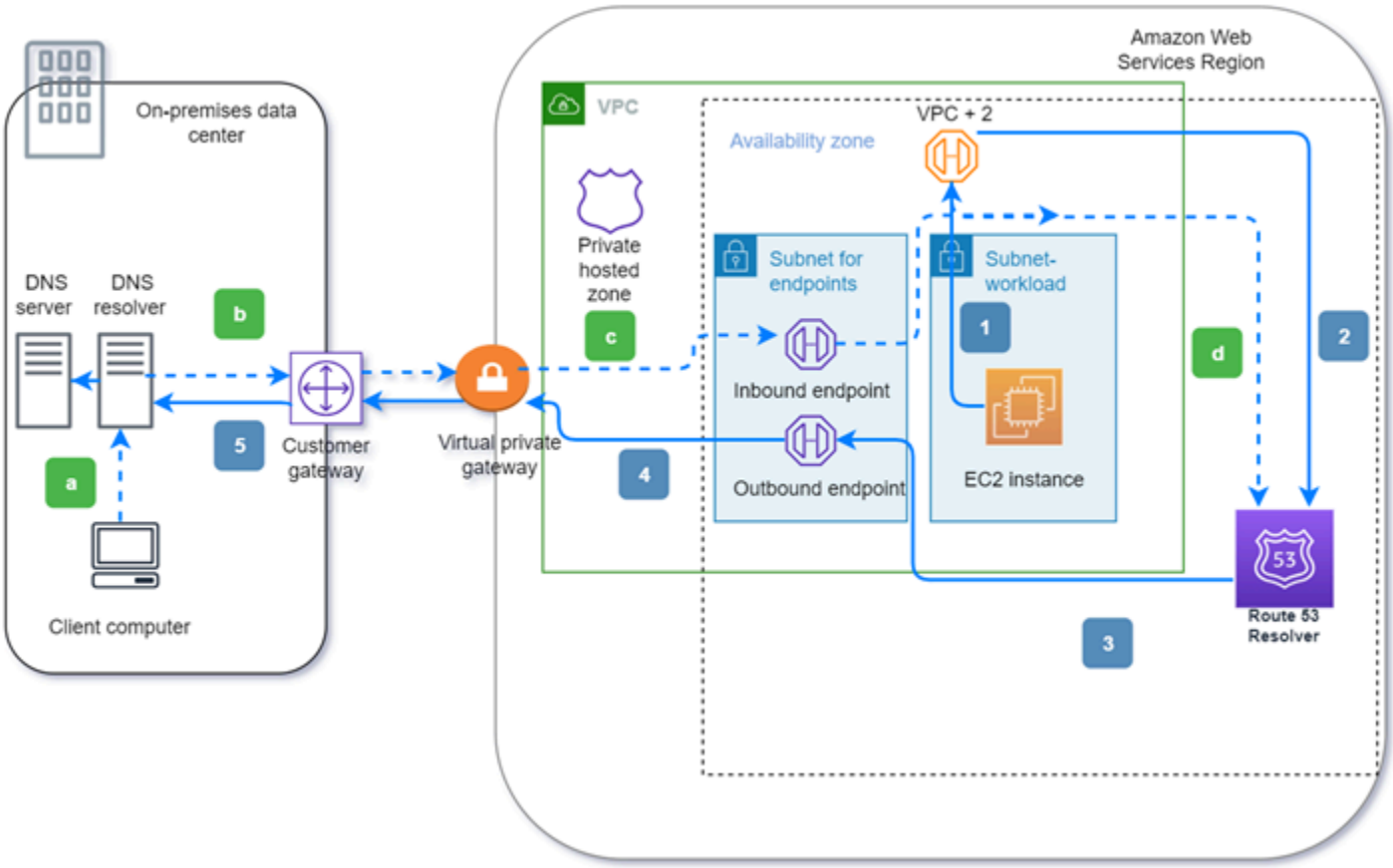
- Nomi di dominio VPC locali per le EC2 istanze (ad esempio, ec2-192-0-2-44.compute-1.amazonaws.com).
- Record in zone ospitate private (ad esempio acme.esempio.com).
- Per i nomi di domini pubblici, Route 53 Resolver esegue ricerche ricorsive di tutti i server nomi pubblici su Internet.

Se disponi di carichi di lavoro che sfruttano sia le risorse locali che quelle locali, devi risolvere anche i record DNS ospitati in locale. VPCs Analogamente, queste risorse locali potrebbero dover risolvere i nomi ospitati su. AWS Tramite gli endpoint Resolver e le regole di inoltro condizionale, puoi risolvere le query DNS tra le tue risorse locali e creare una configurazione cloud ibrida tramite VPN o VPCs Direct Connect (DX). Nello specifico:

- Gli endpoint di Resolver in entrata consentono query DNS al VPC dalla rete on-premise o da un altro VPC.
- Gli endpoint di Resolver in uscita consentono query DNS al VPC dalla rete on-premise o da un altro VPC.

- Le regole di Resolver consentono di creare una regola di inoltro per ogni nome dominio e specificare il nome del dominio per cui inoltrare query DNS dal VPC a un risolutore DNS on-premise e dalle risorse on-premise al VPC. Le regole vengono applicate direttamente al VPC e possono essere condivise tra più account.

Il diagramma seguente mostra la risoluzione DNS ibrida con endpoint di Resolver. Tieni presente che il diagramma è semplificato e mostra una sola zona di disponibilità.



Il diagramma illustra i passaggi seguenti:

In uscita (frecce piene 1 5):

1. Un' EC2 istanza Amazon deve risolvere una query DNS sul dominio internal.example.com. Il server DNS autorevole è collocato nel data center on-premise. Questa query DNS viene inviata al VPC+2 nel VPC che si connette a Route 53 Resolver.
2. Una regola di inoltro di Route 53 Resolver è configurata per l'inoltro delle query a internal.esempio.com nel data center on-premise.
3. La query viene inoltrata a un endpoint in uscita.

4. L'endpoint in uscita inoltra la query al resolver DNS locale tramite una connessione privata tra e il data center. AWS La connessione può essere rappresentata AWS Direct Connect o rappresentata come un gateway privato AWS Site-to-Site VPN virtuale.
5. Il resolver DNS locale risolve la query DNS per internal.example.com e restituisce la risposta all'istanza Amazon tramite lo stesso percorso al contrario. EC2

In entrata (frecce tratteggiate a—d):

a. Un client nel data center locale deve risolvere una query DNS su una risorsa per il dominio dev.example.com. AWS Invia la query al risolutore DNS locale on-premise.
b. Il risolutore DNS on-premise ha una regola di inoltro che indirizza le query a dev.esempio.com a un endpoint in entrata.
c. La query arriva all'endpoint in entrata tramite una connessione privata, ad esempio o, rappresentata come AWS Direct Connect un gateway virtuale. AWS Site-to-Site VPN
d. L'endpoint in ingresso invia la query a Route 53 Resolver e Route 53 Resolver risolve la query DNS per dev.example.com e restituisce la risposta al client tramite lo stesso percorso in senso inverso.

Argomenti

Risoluzione VPCs delle query DNS tra e la rete

Il Resolver contiene endpoint configurati per rispondere alle query DNS da e verso l'ambiente on-premise.

> **Note**
>
> L'inoltro di query DNS private a qualsiasi indirizzo CIDR + 2 del VPC dai server DNS on-premise non è supportato e può causare risultati instabili. Ti consigliamo invece di utilizzare un endpoint in entrata del risolutore.

È inoltre possibile integrare la risoluzione DNS tra il Resolver e i resolver DNS nella rete configurando le regole di inoltro. La rete può includere qualsiasi rete raggiungibile dal VPC, ad esempio:

- Il VPC stesso
- Un altro VPC con peering
- Una rete locale connessa a AWS Direct Connect, una VPN o AWS un gateway NAT (Network Address Translation)

Prima di iniziare a inoltrare le query, è possibile creare endpoint di Resolver in ingresso e/o in uscita nel VPC connesso. Questi endpoint forniscono un percorso per le query in ingresso o in uscita:

Endpoint in ingresso: i resolver DNS nella rete possono inoltrare query DNS a Route 53 Resolver tramite questo endpoint

Ciò consente ai resolver DNS di risolvere facilmente i nomi di dominio per AWS risorse come EC2 istanze o record in una zona ospitata privata di Route 53. Per ulteriori informazioni, consulta Come i resolver DNS sulla rete inoltrano query DNS agli endpoint di Route 53 Resolver .

Endpoint in uscita: il Resolver inoltra in modo condizionale le query ai resolver sulla rete tramite questo endpoint

Per inoltrare le query selezionate, devi creare regole di Resolver che specifichino i nomi di dominio per le query DNS da inoltrare (ad esempio esempio.com) e gli indirizzi IP dei resolver DNS sulla rete ai quali inoltrare le query. Se una query corrisponde a più regole (esempio.com, acme.esempio.com), il Resolver sceglie la regola con la corrispondenza più specifica (acme.esempio.com) e inoltra la query agli indirizzi IP specificati in quella regola. Per ulteriori informazioni, consulta In che modo l'endpoint Route 53 Resolver inoltra le query DNS dall'utente alla rete VPCs .

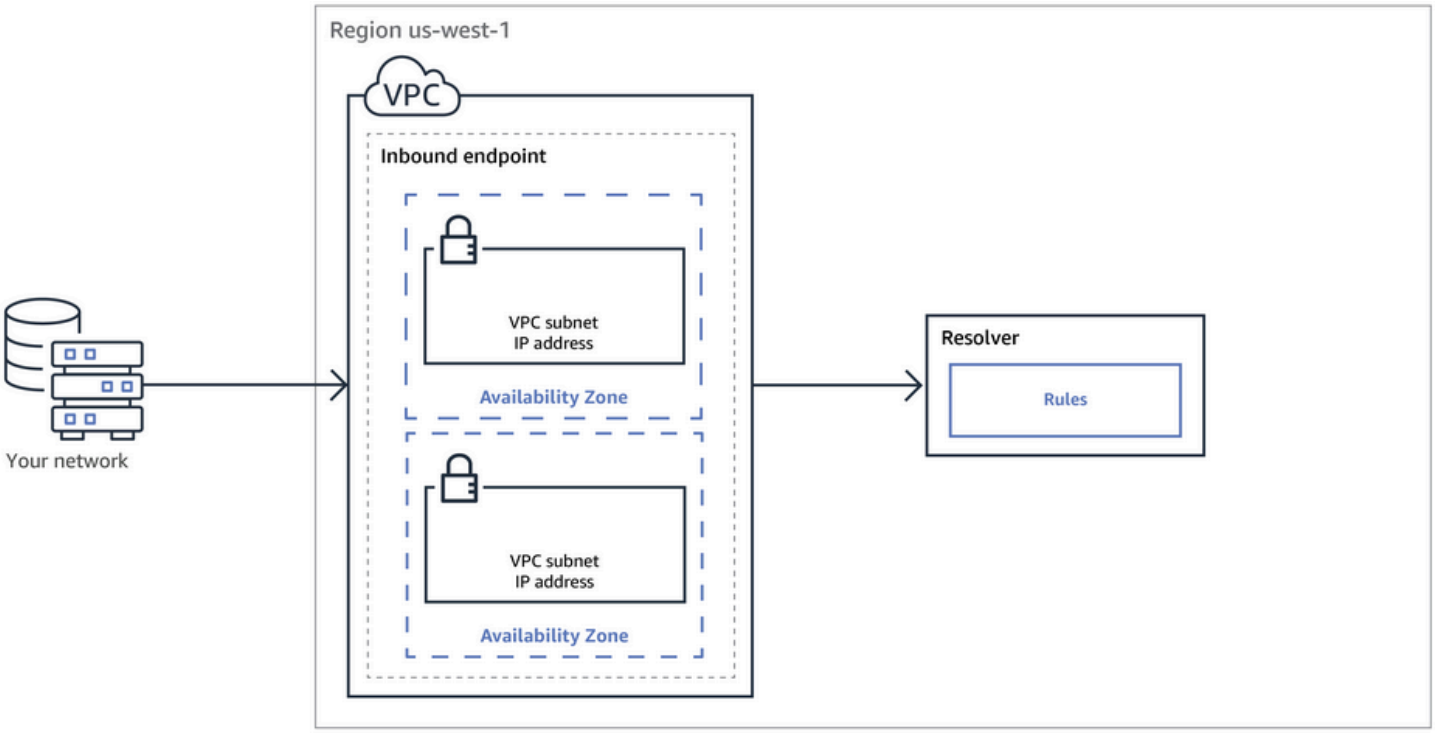
Come Amazon VPC, il Resolver è regionale. In ogni regione in cui ti trovi VPCs, puoi scegliere se inoltrare le interrogazioni dalla tua rete VPCs alla tua rete (query in uscita), dalla rete alla tua VPCs (query in entrata) o entrambe.

Non puoi creare endpoint Resolver in un VPC che non sono di tua proprietà. Solo il proprietario del VPC può creare risorse a livello di VPC, ad esempio gli endpoint in ingresso.

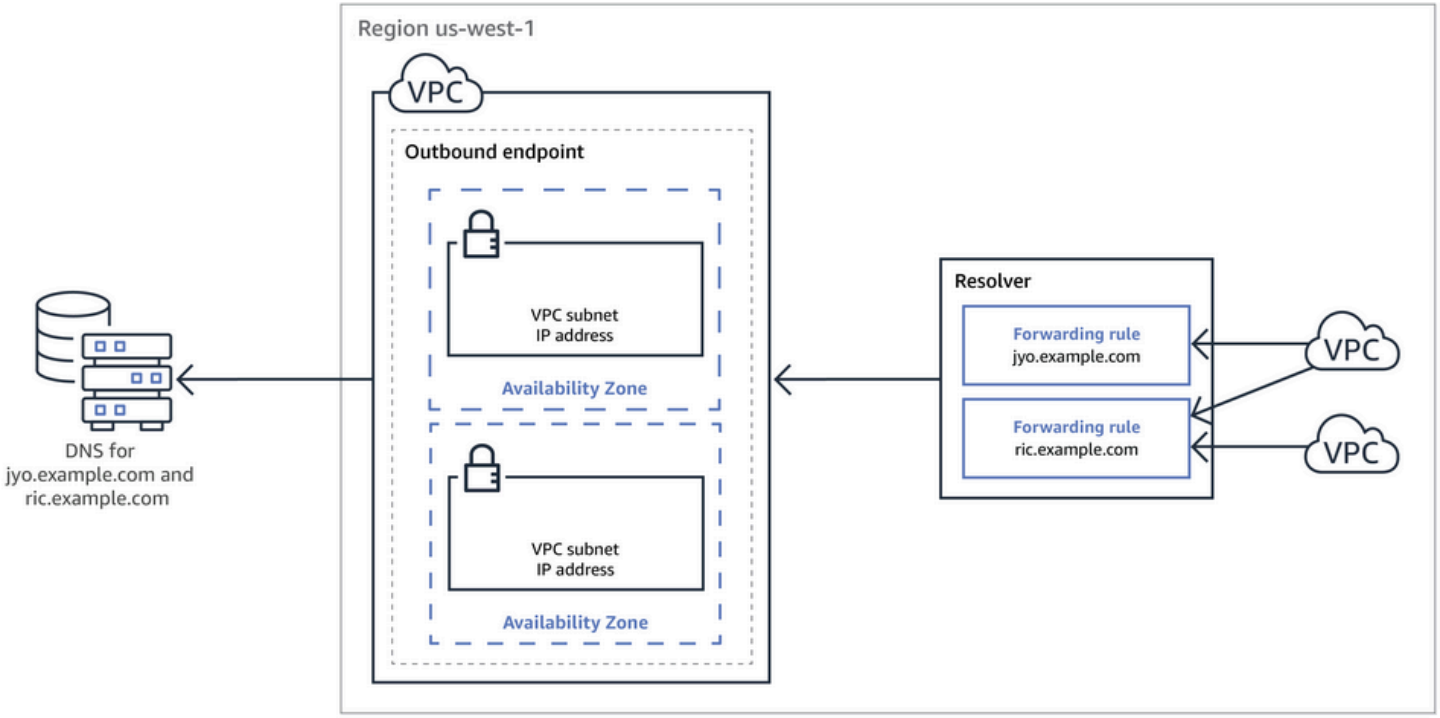
> **Note**
>
> Quando crei un endpoint Resolver, non è possibile specificare un VPC con l'attributo di tenancy dell'istanza impostato su `dedicated`. Per ulteriori informazioni, consulta .

Per utilizzare l'inoltro in entrata o in uscita, crea un endpoint Resolver nel VPC. In quanto parte della definizione di un endpoint, è necessario specificare gli indirizzi IP a cui si desidera inoltrare le query DNS in entrata o gli indirizzi IP da cui si desidera provengano le query in uscita. Per ogni indirizzo IP specificato, Resolver crea automaticamente un'interfaccia di rete elastica VPC.

Il seguente diagramma mostra il percorso di una query DNS da un resolver DNS sulla rete agli endpoint di Resolver Route 53.



Il diagramma seguente mostra il percorso di una query DNS da un' EC2 istanza di uno di voi a un resolver DNS sulla rete VPCs .



Per una panoramica delle interfacce di rete VPC, consulta Interfaccia di rete elastica nella Guida per l'utente di Amazon VPC.

Argomenti

- Come i resolver DNS sulla rete inoltrano query DNS agli endpoint di Route 53 Resolver
- In che modo l'endpoint Route 53 Resolver inoltra le query DNS dall'utente alla rete VPCs
- Considerazioni per la creazione di endpoint in entrata e in uscita

Come i resolver DNS sulla rete inoltrano query DNS agli endpoint di Route 53 Resolver

Se desideri inoltrare query DNS dalla tua rete agli endpoint di Route 53 Resolver in una Regione AWS , procedi come segue:

1. Crea un endpoint in entrata Route 53 Resolver in un VPC e specifica gli indirizzi IP a cui i resolver sulla rete inoltrano le query DNS.

   Per ogni indirizzo IP specificato per l'endpoint in entrata, Resolver crea un'interfaccia di rete elastica VPC nel VPC in cui è stato creato l'endpoint in entrata.

2. Configura i resolver sulla rete in modo che inoltrino query DNS per i nomi di dominio applicabili agli indirizzi IP specificati nell'endpoint in entrata. Per ulteriori informazioni, consulta Considerazioni per la creazione di endpoint in entrata e in uscita.

Ecco come Resolver risolve le query DNS che sono originate nella tua rete:

1. Un browser Web o a un'altra applicazione sulla rete invia una query DNS per un nome di dominio inoltrato a Resolver.
2. Un resolver sulla rete inoltra la query agli indirizzi IP dell'endpoint in entrata.
3. L'endpoint in entrata inoltra la query a Resolver.
4. Resolver ottiene il valore applicabile per il nome di dominio nella query DNS, internamente o eseguendo una ricerca ricorsiva dei server dei nomi pubblici.
5. Il resolver restituisce il valore all'endpoint in entrata.
6. L'endpoint in entrata restituisce il valore al resolver sulla rete.
7. Il resolver sulla rete restituisce il valore all'applicazione.
8. Utilizzando il valore stato restituito da Resolver, l'applicazione invia una richiesta HTTP, ad esempio una richiesta per un oggetto in un bucket Amazon S3.

La creazione di un endpoint in entrata non modifica il comportamento di Resolver, ma fornisce semplicemente un percorso da una posizione esterna alla rete a Resolver. AWS

In che modo l'endpoint Route 53 Resolver inoltra le query DNS dall'utente alla rete VPCs

Per inoltrare le query DNS dalle EC2 istanze di una o più AWS regioni alla rete, procedi VPCs nel seguente modo.

1. Crea un endpoint in uscita di Route 53 Resolver in un VPC e specifica diversi valori:
   - Il VPC nel quale vuoi che le query DNS passino in direzione dei resolver sulla rete.
   - Gli indirizzi IP nel VPC a cui Resolver deve inoltrare le query DNS. Per gli host sulla rete, questi sono gli indirizzi IP da cui originano le query DNS.
   - Un gruppo di sicurezza VPC

Per ogni indirizzo IP specificato per l'endpoint di uscita, Resolver crea un'interfaccia di rete elastica di Amazon VPC nel VPC specificato. Per ulteriori informazioni, consulta Considerazioni per la creazione di endpoint in entrata e in uscita.

2. Crea una o più regole che specifichino i nomi di dominio delle query DNS che desideri siano inoltrate da Resover ai resolver sulla rete. Specifica anche gli indirizzi IP dei resolver. Per ulteriori informazioni, consulta Utilizzo di regole per controllare quali query vengono inoltrate alla rete.
3. Associate ogni regola a quella VPCs per cui desiderate inoltrare le query DNS alla rete.

Argomenti

Utilizzo di regole per controllare quali query vengono inoltrate alla rete

Le regole controllano quali query DNS vengono inoltrate dall'endpoint di Route 53 Resolver ai resolver DNS sulla rete e a quali risponde direttamente Resolver.

Puoi categorizzare le regole in due modi. Un modo è basato su chi crea le regole:

- Regole autodefinite: Resolver crea automaticamente regole autodefinite e le associa alle tue. VPCs La maggior parte di queste regole si applica ai nomi di dominio AWS specifici per i quali Resolver risponde alle domande. Per ulteriori informazioni, consulta Nomi di dominio per cui Resolver crea regole di sistema autodefinite.
- Regole personalizzate: crei regole personalizzate e le associ a. VPCs Al momento è possibile creare solo un tipo di regole personalizzate, le regole di inoltro condizionale, anche dette regole di inoltro. Le regole di inoltro fanno sì che Resolver inoltri le query DNS dall'utente VPCs agli indirizzi IP per i resolver DNS sulla rete.

  Se crei una regola di inoltro per lo stesso dominio di una regola autodefinita, Resolver inoltra le query per quel nome di dominio ai resolver DNS sulla rete in base alle impostazioni della regola di inoltro.

L'altro modo per categorizzare le regole è in base ai loro effetti:

- Regole di inoltro condizionali: è possibile creare regole di inoltro condizionale (note anche come regole di inoltro) quando vuoi inoltrare query DNS per i nomi di dominio specificati ai resolver DNS sulla rete.
- Regole di sistema: le regole di sistema fanno sì che Resolver sostituisca in modo selettivo il comportamento definito in una regola di inoltro. Quando crei una regola di sistema, Resolver risolve le query DNS per sottodomini specificati che altrimenti verrebbero risolti dai resolver DNS sulla rete.

  Per impostazione predefinita, le regole di inoltro valgono per un nome di dominio e per tutti i relativi sottodomini. Se vuoi inoltrare le query per un dominio a un resolver sulla rete ma non vuoi inoltrare query per alcuni sottodomini, devi creare una regola di sistema per i sottodomini. Ad esempio, se crei una regola di inoltro per esempio.com ma non vuoi inoltrare query per acme.esempio.com, devi creare una regola di sistema e specificare acme.esempio.com come nome di dominio.
- Regola ricorsiva: Resolver crea automaticamente una regola ricorsiva denominata Resolver di Internet. Questa regola consente a Route 53 Resolver di funzionare come resolver ricorsivo per tutti i nomi di dominio per i quali non sono state create regole personalizzate e per i quali Resolver non ha creato regole autodefinite. Per informazioni su come ignorare questo comportamento, consulta la sezione "Inoltrare tutte le query alla rete" più avanti in questo argomento.

Puoi creare regole personalizzate che si applicano a nomi di dominio specifici (i tuoi o la maggior parte dei nomi di dominio), ai nomi di AWS dominio pubblici o a tutti i nomi di dominio. AWS

Inoltro di query per nomi di dominio specifici alla rete

Per inoltrare query per un nome di dominio specifico, come esempio.com, alla rete, devi creare una regola e specificare il nome di dominio. Devi anche specificare gli indirizzi IP dei resolver DNS sulla rete a cui vuoi inoltrare le query. Quindi associ ogni regola a quella VPCs per cui desideri inoltrare le query DNS alla tua rete. Ad esempio, è possibile creare regole separate per esempio.com, esempio.org ed esempio.net. È quindi possibile associare le regole a quelle di una AWS regione VPCs in qualsiasi combinazione.

Inoltro di query per amazonaws.com alla rete

Il nome di dominio amazonaws.com è il nome di dominio pubblico per AWS risorse come EC2 istanze e bucket S3. Se vuoi inoltrare le query per amazonaws.com alla rete, crea una regola, specifica amazonaws.com come nome di dominio e specifica Forward (Inoltro) per il tipo di regola.

> **Note**
>
> Resolver non inoltra automaticamente query DNS per alcuni sottodomini di amazonaws.com, neanche se crei una regola di inoltro per amazonaws.com. Per ulteriori informazioni, consulta Nomi di dominio per cui Resolver crea regole di sistema autodefinite. Per informazioni su come ignorare questo comportamento, consulta la sezione immediatamente successiva "Inoltrare tutte le query alla rete".

Inoltrare tutte le query alla rete

Se desideri inoltrare tutte le query alla tua rete, crea una regola, specifica «.» (punto) per il nome di dominio e associa la regola alla VPCs quale desideri inoltrare tutte le query DNS alla tua rete. Resolver continua a non inoltrare tutte le query DNS alla rete perché l'utilizzo di un resolver DNS esterno comprometterebbe alcune funzionalità. AWS Ad esempio, alcuni nomi di AWS dominio interni hanno intervalli di indirizzi IP interni che non sono accessibili dall'esterno di. AWS Per un elenco dei nomi di dominio per i quali le query non vengono inoltrate alla rete quando crei una regola per ".", consulta Nomi di dominio per cui Resolver crea regole di sistema autodefinite.

Tuttavia, le regole di sistema definite automaticamente per il DNS inverso possono essere disabilitate, consentendo alla regola «.» di inoltrare tutte le query DNS inverse alla rete. Per ulteriori informazioni su come disattivare le regole autodefinite, consultare Regole di inoltro per le query DNS inverse in Resolver.

Se vuoi provare a inoltrare query DNS per tutti i nomi di dominio alla rete, compresi i nomi di dominio esclusi dall'inoltro per impostazione predefinita, puoi creare una regola "." e procedere in uno dei seguenti modi:

- Impostando il flag `enableDnsHostnames` per il VPC su `false`
- Creando regole per i nomi di dominio elencati in Nomi di dominio per cui Resolver crea regole di sistema autodefinite

> **Important**
>
> Se inoltri tutti i nomi di dominio alla rete, compresi i nomi di dominio esclusi dal Resolver quando crei una regola ".", alcune funzionalità potrebbero smettere di funzionare.

Come Resolver determina se il nome di dominio in una query corrisponde alle regole

Route 53 Resolver confronta il nome di dominio nella query DNS con il nome di dominio nelle regole associate al VPC da cui è stata originata la query. Resolver considera che i nomi di dominio corrispondano nei seguenti casi:

- I nomi di dominio corrispondono esattamente
- Il nome di dominio nella query è un sottodominio del nome di dominio nella regola

Ad esempio, se il nome di dominio nella regola è acme.esempio.com, Resolver considera i seguenti nomi di dominio in una query DNS come corrispondenti:

- acme.esempio.com
- zenith.acme.esempio.com

I seguenti nomi di dominio non sono una corrispondenza:

- esempio.com
- nadir.esempio.com

Se il nome di dominio in una query corrisponde al nome di dominio in più di una regola (come esempio.com e www.esempio.com), Resolver instrada le query DNS in uscita utilizzando la regola che contiene il nome di dominio più specifico (www.esempio.com).

In che modo Resolver determina dove inoltrare le query DNS

Quando un'applicazione eseguita su un' EC2 istanza in un VPC invia una query DNS, Route 53 Resolver esegue i seguenti passaggi:

1. Il resolver controlla i nomi di dominio nelle regole.

   Se il nome di dominio in una query corrisponde al nome di dominio in una regola, Resolver inoltra la query all'indirizzo IP specificato al momento della creazione dell'endpoint in uscita. L'endpoint in uscita inoltra quindi la query agli indirizzi IP dei resolver sulla rete, da te indicati al momento della creazione della regola.

   Per ulteriori informazioni, consulta Come Resolver determina se il nome di dominio in una query corrisponde alle regole.

2. L'endpoint di Resolver inoltre le query DNS in base alle impostazioni nella regola ".".

   Se il nome di dominio in una query non corrisponde al nome di dominio in qualsiasi altra regola, Resolver inoltra la query in base alle impostazione nella regola autodefinita "." (punto). La regola del punto si applica a tutti i nomi di dominio ad eccezione di alcuni nomi di dominio AWS interni e nomi di record nelle zone ospitate private. Questa regola permette a Resolver di inoltrare query DNS ai server di nomi pubblici se i nomi di dominio nelle query non corrispondono ai nomi nelle regole di inoltro personalizzate. Se vuoi inoltrare tutte le query ai resolver DNS sulla rete, puoi creare una regola di inoltro personalizzata, specificare "." per il nome di dominio, specificare Forwarding (Inoltro) per Type (Tipo) e specificare gli indirizzi IP di questi resolver.

3. Resolver restituisce la risposta all'applicazione che ha inviato la query.

Utilizzo di regole in più regioni

Route 53 Resolver è un servizio regionale, quindi gli oggetti creati in una AWS regione sono disponibili solo in quella regione. Per utilizzare la stessa regola in più di una regione, è necessario creare la regola in ciascuna regione.

L' AWS account che ha creato una regola può condividerla con altri AWS account. Per ulteriori informazioni, consulta Condivisione delle regole del Resolver con altri AWS account e utilizzo di regole condivise.

Nomi di dominio per cui Resolver crea regole di sistema autodefinite

Il resolver crea automaticamente regole di sistema autodefinite che definiscono la modalità predefinita utilizzata per risolvere le query per i domini selezionati:

- Per le zone ospitate private e per i nomi di dominio EC2 specifici di Amazon (come compute.amazonaws.com e compute.internal), le regole definite automaticamente assicurano che le zone e le EC2 istanze ospitate private continuino a risolversi se crei regole di inoltro condizionale per nomi di dominio meno specifici come «.» (dot) o «com».
- Per i nomi di dominio riservati pubblicamente (come localhost e 10.in-addr.arpa), le best practice DNS consigliano che le query vengano risposte a livello locale invece che inoltrate ai server di nomi pubblici. Consulta RFC 6303, zone DNS servite localmente.

> **Note**
>
> Se crei una regola di inoltro condizionale per "." (punto) o "com", ti consigliamo di creare anche una regola di sistema per amazonaws.com. (Le regole di sistema fanno si che Resolver risolva le query DNS in locale per domini e sottodomini specifici.) La creazione di questa regola di sistema migliora le prestazioni, riduce il numero di query che vengono inoltrate alla rete e riduce i costi di Resolver.

Se desideri sostituire una regola autodefinita, puoi creare una regola di inoltro condizionale per lo stesso nome di dominio.

Puoi anche disabilitare alcune delle regole definite automaticamente. Per ulteriori informazioni, consulta Regole di inoltro per le query DNS inverse in Resolver.

Il resolver crea le seguenti regole autodefinite.

Regole per zone ospitate private

Per ogni zona ospitata privata che viene associata a un VPC, Resolver crea una regola e la associa al VPC. Se associ la zona ospitata privata a più zone VPCs, Resolver associa la regola alle stesse. VPCs

La regola è di tipo Forward (Inoltro).

Regole per vari nomi di dominio interni AWS

Tutte le regole per i nomi di dominio interni in questa sezione sono di tipo Forward. Resolver inoltra query DNS per questi nomi di dominio ai server di nomi ufficiali del VPC.

> **Note**
>
> Resolver crea la maggior parte di queste regole quando si imposta l'indicatore `enableDnsHostnames` per un VPC su `true`. Resolver crea le regole anche se non utilizzi endpoint Resolver.

Resolver crea le seguenti regole autodefinite e le associa a un VPC quando imposti l'indicatore `enableDnsHostnames` per il VPC su `true`:

- *Region-name*.compute.internal, ad esempio eu-west-1.compute.internal. La regione us-east-1 non utilizza questo nome di dominio.
- *Region-name*.calcolare. *amazon-domain-name*, ad esempio, eu-west-1.compute.amazonaws.com o cn-north-1.compute.amazonaws.com.cn. La regione us-east-1 non utilizza questo nome di dominio.
- ec2.internal. Solo la regione us-east-1 utilizza questo nome di dominio.
- compute-1.internal. Solo la regione us-east-1 utilizza questo nome di dominio.
- compute-1.amazonaws.com. Solo la regione us-east-1 utilizza questo nome di dominio.

Le seguenti regole autodefinite valgono per la ricerca DNS inversa per le regole create da Resolver quando imposti l'indicatore `enableDnsHostnames` per il VPC su `true`.

- 10.in-addr.arpa
- Da 16.172.in-addr.arpa a 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Regole di ciascuna delle gamme CIDR per il VPC. Ad esempio, se un VPC ha una gamma di CIDR 10.0.0.0/23, Resolver crea le seguenti regole:
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

Anche le seguenti regole autodefinite, per i domini correlati ai localhost, vengono create e associate a un VPC quando imposti il flag `enableDnsHostnames` per il VPC su `true`:

- 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 crea le seguenti regole autodefinite e le associa al VPC quando colleghi il VPC a un altro VPC tramite gateway di transito o peering VPC e con il supporto DNS abilitato:

- La ricerca DNS inversa per gli intervalli di indirizzi IP del VPC in peering, ad esempio 0.192.in-addr.arpa

  Se aggiungi un blocco IPv4 CIDR a un VPC, Resolver aggiunge una regola definita automaticamente per il nuovo intervallo di indirizzi IP.

- Se l'altro VPC si trova in un'altra regione, i seguenti nomi di dominio:
  - *Region-name*.compute.interno. La regione us-east-1 non utilizza questo nome di dominio.
  - *Region-name*.calcolare. *amazon-domain-name*. La regione us-east-1 non utilizza questo nome di dominio.
  - ec2.internal. Solo la regione us-east-1 utilizza questo nome di dominio.
  - compute-1.amazonaws.com. Solo la regione us-east-1 utilizza questo nome di dominio.

Una regola per tutti gli altri domini

Resolver crea una regola "." (punto) valida per tutti i nomi di dominio non specificati prima in questo argomento. La regola "." è di tipo ricorsivo, il che significa che fa in modo che Resolver agisca da resolver ricorsivo.

Considerazioni per la creazione di endpoint in entrata e in uscita

Prima di creare endpoint Resolver in entrata e in uscita in una AWS regione, considerate i seguenti problemi.

Argomenti

Numero di endpoint in entrata e in uscita in ciascuna regione

Quando desideri integrare il DNS di una AWS regione con il DNS della tua rete, VPCs in genere hai bisogno di un endpoint Resolver in entrata (per le query DNS che stai inoltrando alla tua VPCs) e un endpoint in uscita (per le query che stai inoltrando dalla tua rete). VPCs Puoi creare più endpoint in

entrata e più endpoint in uscita, ma un endpoint in entrata o in uscita è sufficiente per gestire le query DNS per ogni rispettiva direzione. Tieni presente quanto segue:

- Per ogni endpoint di Resolver, è necessario specificare due o più indirizzi IP in diverse zone di disponibilità. Ogni indirizzo IP in un endpoint è in grado di gestire un numero elevato di query DNS al secondo. (Per quanto riguarda il numero massimo di query al secondo per indirizzo IP in un endpoint, consulta Quote relative a Route 53 Resolver). Se è necessario che Resolver gestisca più query, invece di aggiungere un altro endpoint puoi aggiungere altri indirizzi IP all'endpoint esistente.
- I prezzi di Resolver sono calcolati in base al numero di indirizzi IP negli endpoint e sul numero di query DNS elaborate dall'endpoint. Ogni endpoint include almeno due indirizzi IP. Per ulteriori informazioni sui prezzi di Resolver, consulta Prezzi di Amazon Route 53.
- Ogni regola specifica l'endpoint in uscita da cui vengono inoltrate le query DNS. Se crei più endpoint in uscita in una regione AWS e desideri associare alcune o tutte le regole di Resolver a ogni VPC, è necessario creare più copie di tali regole.

Utilizzare lo stesso VPC per gli endpoint in entrata e in uscita

È possibile creare endpoint in entrata e in uscita nello stesso VPC o in diversi VPCs punti della stessa regione.

Per ulteriori informazioni, consulta Best practice per Amazon Route 53.

Endpoint in entrata e zone ospitate private

Se desideri che Resolver risolva le query DNS in entrata utilizzando i record in una zona ospitata privata, associa la zona ospitata privata al VPC in cui è stato creato l'endpoint in entrata. Per informazioni sull'associazione di zone ospitate private a, consulta. VPCs Utilizzo delle zone ospitate private

Peering VPC

Puoi utilizzare qualsiasi VPC in una AWS regione per un endpoint in entrata o in uscita indipendentemente dal fatto che il VPC scelto sia peerizzato con altri. VPCs Per ulteriori informazioni, consulta la sezione relativa al peering Amazon Virtual Private Cloud (VPC).

Indirizzi IP nelle sottoreti condivise

Quando si crea un endpoint in ingresso o in uscita, è possibile specificare un indirizzo IP in una subnet condivisa solo se l'account corrente ha creato il VPC. Se un altro account crea un VPC e condivide una subnet nel VPC con l'account, non è possibile specificare un indirizzo IP in tale subnet. Per ulteriori informazioni sulle sottoreti condivise, consulta Working with shared VPCs nella Amazon VPC User Guide.

Connessione tra la tua rete e VPCs quella in cui crei gli endpoint

È necessario disporre di una delle seguenti connessioni tra la rete e VPCs quella in cui vengono creati gli endpoint:

- Endpoint in entrata: devi configurare una connessione AWS Direct Connect o una connessione VPN tra la tua rete e ciascun VPC per cui crei un endpoint in entrata o in uscita.
- Endpoint in uscita: è necessario configurare una connessione AWS Direct Connect, una connessione VPN o un gateway NAT (network address translation) tra la rete e ogni VPC per il quale è stato creato un endpoint in uscita.

Quando si condividono le regole, si condividono anche gli endpoint in uscita

Quando crei una regola, è necessario specificare l'endpoint in uscita che si desidera sia utilizzato da Resolver per inoltrare query DNS alla rete. Se condividi la regola con un altro AWS account, condividi anche indirettamente l'endpoint in uscita specificato nella regola. Se hai utilizzato più di un AWS account per creare VPCs in una AWS regione, puoi fare quanto segue:

- Creare un endpoint in uscita nella regione.
- Crea regole utilizzando un solo AWS account.
- Condividi le regole con tutti gli AWS account creati VPCs nella Regione.

Ciò consente di utilizzare un endpoint in uscita in una regione per inoltrare le query DNS alla rete da più utenti, VPCs anche se VPCs sono state create utilizzando account diversi. AWS

Scelta dei protocolli per gli endpoint

I protocolli degli endpoint determinano il modo in cui i dati vengono trasmessi a un endpoint in entrata e da un endpoint in uscita. La crittografia delle query DNS per il traffico VPC non è necessaria

perché ogni flusso di pacchetti nella rete viene autorizzato individualmente in base a una regola per convalidare l'origine e la destinazione corrette prima della sua trasmissione e consegna. È molto improbabile che le informazioni vengano trasmesse in modo arbitrario tra entità senza che siano specificamente autorizzate sia dall'entità trasmittente che da quella ricevente. Se viene indirizzato a una destinazione priva di una regola corrispondente, un pacchetto viene eliminato. Per ulteriori informazioni, consulta le funzionalità del VPC.

I protocolli disponibili sono:

- Do53: DNS sulla porta 53. I dati vengono inoltrati utilizzando Route 53 Resolver senza crittografia aggiuntiva. Sebbene i dati non possano essere letti da soggetti esterni, possono essere visualizzati all'interno delle reti. AWS Utilizza UDP o TCP per inviare i pacchetti. Do53 viene utilizzato principalmente per il traffico all'interno e tra Amazon VPCs.
- DoH: i dati vengono trasmessi attraverso una sessione HTTPS crittografata. DoH aggiunge un ulteriore livello di sicurezza in cui i dati non possono essere decrittografati da utenti non autorizzati né letti da nessuno all'infuori del destinatario previsto.
- DoH-FIPS: i dati vengono trasmessi attraverso una sessione HTTPS crittografata conforme allo standard di crittografia FIPS 140-2. Supportato solo per gli endpoint in entrata. Per ulteriori informazioni, consulta FIPS PUB 140-2.

Per un endpoint in entrata, è possibile applicare i protocolli come segue:

- Do53 e DoH in combinazione.
- Do53 e DoH-FIPS in combinazione.
- Do53 da solo.
- DoH da solo.
- DoH-FIPS da solo.
- Nessuno, il che equivale a Do53.

Per un endpoint in uscita è possibile applicare i protocolli come segue:

- Do53 e DoH in combinazione.
- Do53 da solo.
- DoH da solo.
- Nessuno, il che equivale a Do53.

Consulta anche Valori specificati durante la creazione o la modifica di endpoint in entrata e Valori specificati durante la creazione o la modifica degli endpoint in uscita.

Utilizzo di Resolver in quanto configurati per VPCs la locazione di istanze dedicate

Quando crei un endpoint Resolver, non è possibile specificare un VPC con l'attributo di tenancy dell'istanza impostato su `dedicated`. Resolver non viene eseguito su hardware a tenant singolo.

Puoi comunque utilizzare Resolver per risolvere le query DNS che hanno origine in un VPC. Crea almeno un VPC che abbia l'attributo di tenancy dell'istanza impostato su `default` e specifica quel VPC al momento della creazione di endpoint in entrata e in uscita.

Quando si crea una regola di inoltro, è possibile associarla a qualsiasi VPC, indipendentemente dall'impostazione dell'attributo di tenancy dell'istanza.

Disponibilità e scalabilità di Route 53 Resolver

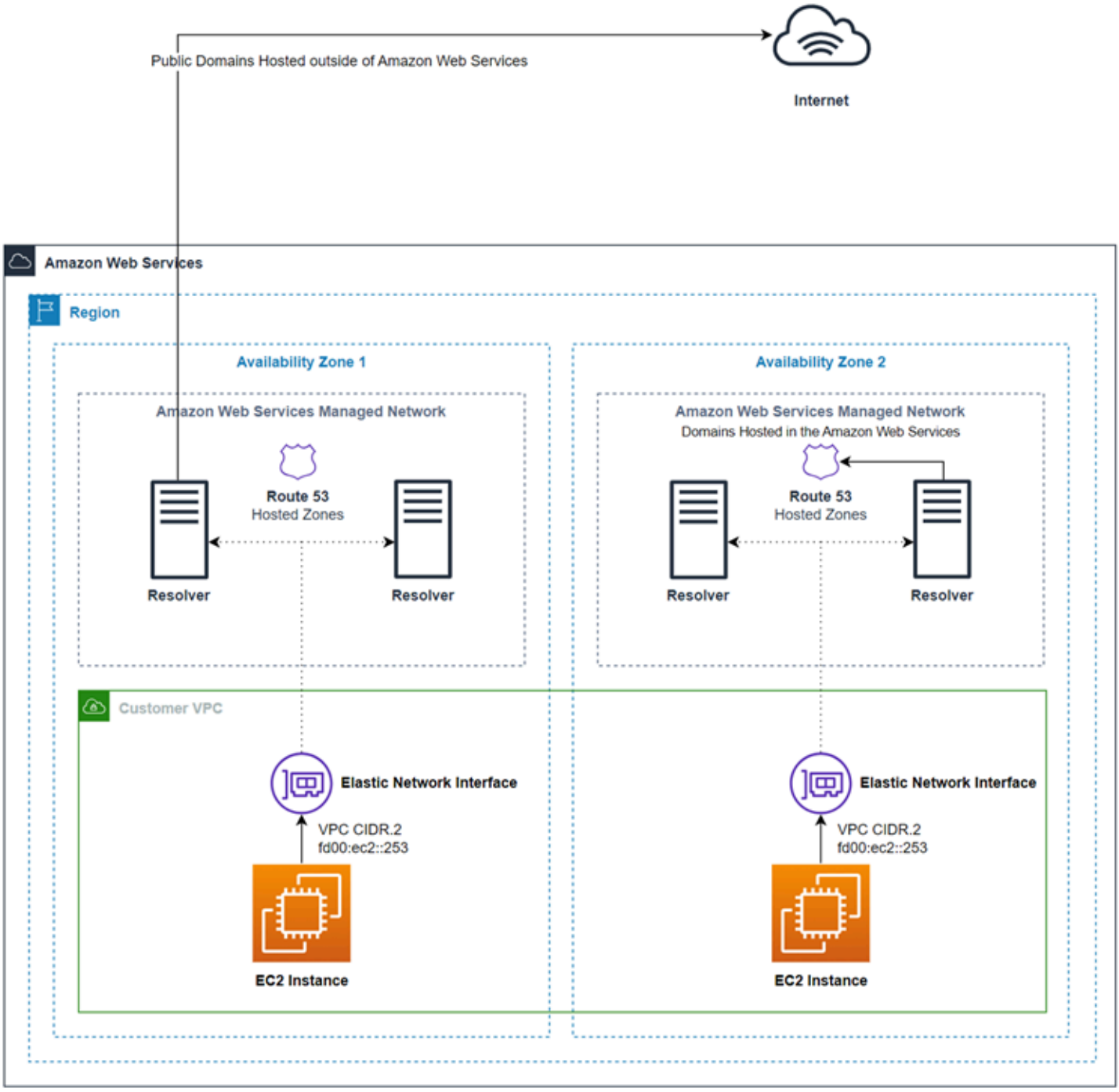
Amazon Route 53 Resolver, in esecuzione sull'indirizzo Amazon VPC CIDR + 2 e fd00:ec2: :253, è disponibile per impostazione predefinita in tutti e risponde in modo ricorsivo alle query DNS per record pubblici VPCs, nomi DNS specifici di Amazon VPC e zone ospitate private Route 53. Esistono due componenti ad alta disponibilità, trasparenti per gli utenti, che compongono il Route 53 Resolver: il servizio Nitro Resolver e la flotta Zonal Resolver. Il servizio Nitro Resolver è un servizio che viene eseguito nella scheda Nitro sulle istanze Nitro e in Dom0 nelle istanze di vecchia generazione e utilizza i pacchetti indirizzati al Route 53 Resolver localmente sul server host. Per ulteriori informazioni, consulta La progettazione della sicurezza del sistema Nitro. AWS

Il servizio Nitro Resolver include una cache locale che può aiutare a ridurre la latenza rispondendo alle domande ripetute che vengono eseguite in un breve periodo di tempo da un'istanza. Quando il servizio Nitro Resolver riceve una query per la quale non dispone di una risposta memorizzata nella cache, inoltra la query al parco Resolver Zonal, un parco di resolver ad alta disponibilità che si trova in genere nella stessa zona di disponibilità dell'istanza. In caso di errori nella gestione delle query da parte dei name server upstream o di altri componenti del percorso, il servizio Nitro Resolver è spesso in grado di gestire questi errori in modo trasparente senza impatto sui carichi di lavoro in esecuzione sull'istanza. Inoltre, se il Resolver rileva timeout di query, connessioni rifiutate o SERVFAILS dai name server del dominio, può rispondere con una risposta memorizzata nella cache oltre il valore Time-To-Live (TTL) per migliorare la disponibilità. Le richieste tra il servizio Nitro Resolver e la flotta Zonal Resolver sono limitate a una rete strettamente controllata al di fuori del VPC del cliente, che è inaccessibile ai clienti e soggetta a rigorosi controlli di sicurezza. Gestendo le richieste tra

il servizio Nitro Resolver e la flotta Zonal Resolver al di fuori del VPC, ai clienti viene impedito di intercettare le query DNS all'interno del proprio VPC. Le query destinate a denominare server esterni attraverseranno la rete Internet pubblica e provengono da indirizzi IP pubblici appartenenti alla flotta di AWS Zonal Resolver. Attualmente non supportiamo l'attributo EDNS0-Client Subnet, il che significa che tutte le query destinate ai name server DNS pubblici non includono informazioni sull'indirizzo IP del cliente di origine.

Il servizio Nitro Resolver fa parte dei servizi Link-Local sull'istanza. I servizi Link-Local includono Route 53 Resolver, Amazon Time Service (NTP), Instance Metadata Service (IMDS) e Windows Licensing Service (per istanze Windows). Questi servizi si adattano a ogni interfaccia di rete elastica che crei nel tuo VPC e ogni interfaccia di rete consente 1024 pacchetti al secondo (PPS) destinati ai servizi Link-Local. I pacchetti che superano questo limite vengono rifiutati. È possibile determinare se è stato superato questo limite in base al `linklocal_allowance_exceeded` valore restituito da ethtool. Per ulteriori informazioni su ethtool, consulta Monitora le prestazioni di rete per la tua EC2 istanza Amazon nella Amazon EC2 User Guide. Questa metrica può anche essere riportata ai CloudWatch parametri dall'agente. CloudWatch Poiché il Route 53 Resolver è implementato per interfaccia di rete, è scalabile e diventa più affidabile man mano che si aggiungono più istanze in più zone di disponibilità. Non esiste un limite aggregato per VPC al numero di query, quindi il Route 53 Resolver può scalare entro i limiti di un VPC, che è intrinsecamente basato sull'utilizzo degli indirizzi di rete (NAU). Per ulteriori informazioni, consulta l'utilizzo degli indirizzi di rete per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

Il diagramma seguente mostra una panoramica di come Route 53 Resolver risolve le query DNS all'interno delle zone di disponibilità.



Nozioni di base su Route 53 Resolver

La console Route 53 Resolver include una procedura guidata che ti assiste nei seguenti passaggi per iniziare a utilizzare Resolver:

- Creazione di endpoint: in entrata, in uscita o entrambi.

- Per gli endpoint in uscita, crea una o più regole di inoltro, che specificano i nomi di dominio per i quali desideri instradare le query DNS alla rete.
- Se hai creato un endpoint in uscita, seleziona il VPC al quale desideri associare le regole.

Come configurare Route 53 Resolver utilizzando la procedura guidata

1. Accedi e apri la console Resolver all'indirizzo. AWS Management Console https://console.aws.amazon.com/route53resolver/
2. Nella pagina Benvenuti in Route 53 Resolver, seleziona Configura endpoint.
3. Nella barra di navigazione, selezionare la regione dove si desidera creare l'endpoint del resolver.
4. In Basic configuration (Configurazione di base), sceglie la direzione in cui inoltrare le query DNS:
   - In entrata e in uscita: la procedura guidata ti introduce alle impostazioni che permettono sia di inoltrare query DNS sulla rete a Resolver in un VPC sia di inoltrare query specifiche (come esempio.com o esempio.net) da un VPC ai resolver sulla rete.
   - Solo in entrata: la procedura guidata ti introduce alle impostazioni che permettono di inoltrare query DNS sulla rete a Resolver in un VPC.
   - Outbound only (Solo in uscita): la procedura guidata ti introduce alle impostazioni che permettono di inoltrare query specifiche da un VPC ai resolver sulla rete.
5. Seleziona Next (Successivo).
6. Se la scelta è stata Inbound and outbound (In entrata e in uscita) o Inbound only (Solo in uscita), immettere i valori validi per la configurazione di un endpoint in entrata. Continua quindi con la fase 7. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica di endpoint in entrata.

   Se la scelta è stata Outbound only (Solo in uscita), passa alla fase 7.
7. Inserisci i valori applicabili alla configurazione di un endpoint in uscita. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica degli endpoint in uscita.
8. Se la scelta è stata Inbound and outbound (In entrata e in uscita) o Outbound only (Solo in uscita), inserisxci i valori validi per la creazione di una regola. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica delle regole.
9. Nella pagina Review and create (Rivedi e crea), conferma che le impostazioni specificate nelle pagine precedenti sono corrette. Se necessario, seleziona Edit (Modifica) per la sezione applicabile e aggiornare le impostazioni. Quando si è soddisfatti delle impostazioni, seleziona Submit (Invia).

> **Note**
>
> La creazione di un endpoint in uscita richiede un paio di minuti. Non è possibile creare un altro endpoint in uscita fino a quando non viene creato il primo.

10. Se vuoi creare più regole, consulta Gestione delle regole di inoltro.
11. Se hai creato un endpoint in entrata, configura i resolver DNS di rete in modo che inoltrino le query DNS applicabili agli indirizzi IP dell'endpoint in entrata. Per ulteriori informazioni, consulta la documentazione relativa alla tua applicazione DNS.

Inoltro di richieste DNS in entrata al tuo VPCs

Per inoltrare le query DNS dalla rete a Resolver, è necessario creare un endpoint in entrata. Un endpoint in ingresso specifica gli indirizzi IP (dall'intervallo di indirizzi IP disponibili per il VPC) a cui i resolver DNS devono inoltrare le query DNS. Questi indirizzi IP non sono indirizzi IP pubblici, quindi per ogni endpoint in entrata devi connettere il tuo VPC alla rete utilizzando una AWS Direct Connect connessione o una connessione VPN.

Argomenti

Configurazione dell'inoltro in entrata

Per creare un endpoint in entrata, procedi nel seguente modo.

Per creare un endpoint in entrata.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, scegli Inbound endpoints (Inbound in entrata).
3. Nella barra di navigazione, scegli la regione dove si desidera creare l'endpoint in entrata.
4. Sceglie Create inbound endpoint (Crea endpoint in entrata).
5. Immetti i valori applicabili. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica di endpoint in entrata.

6. Scegli Create (Crea) .
7. Configurare i resolver DNS di rete in modo che inoltrino le query DNS applicabili agli indirizzi IP dell'endpoint in entrata. Per ulteriori informazioni, consulta la documentazione relativa alla tua applicazione DNS.

Valori specificati durante la creazione o la modifica di endpoint in entrata

Quando crei o modifichi un endpoint in entrata, devi specificare i seguenti valori:

ID Outpost

Se stai creando l'endpoint per un Resolver su un AWS Outposts VPC, questo è l'ID. AWS Outposts

Nome endpoint

Un nome descrittivo che ti consenta di trovare facilmente un endpoint in entrata nel pannello di controllo.

VPC nella regione region-name.

Tutte le query DNS in entrata dalla rete passano per questo VPC in direzione di Resolver.

Gruppo di sicurezza per questo endpoint

L'ID di uno o più gruppi di sicurezza che si desidera utilizzare per controllare l'accesso a questo VPC. Il gruppo di sicurezza specificato deve includere una o più regole in entrata. Le regole in entrata devono autorizzare l'accesso TCP e UDP sulla porta 53. Non puoi modificare questo valore dopo avere creato l'endpoint.

Alcune regole del gruppo di sicurezza consentiranno il tracciamento della connessione e il numero massimo complessivo di query al secondo per indirizzo IP per un endpoint in ingresso può essere pari a 1500. Per evitare il tracciamento delle connessioni causato da un gruppo di sicurezza, vedi Connessioni non tracciate.

> **Note**
>
> Per aggiungere più gruppi di sicurezza, usa il AWS CLI comando. `create-resolver-endpoint` Per ulteriori informazioni, consulta create-resolver-endpoint

Per ulteriori informazioni, consultare Gruppi di sicurezza per il VPC nella Guida per l'utente di Amazon VPC.

Tipo di endpoint

Il tipo di endpoint può essere uno o più IPv4 indirizzi IPv6 IP dual-stack. Per un endpoint dual-stack, l'endpoint avrà entrambi gli IPv6 indirizzi a cui il resolver DNS sulla rete IPv4 può inoltrare la query DNS.

> **Note**
>
> Per motivi di sicurezza, stiamo negando l'accesso diretto al IPv6 traffico dalla rete Internet pubblica a tutti gli indirizzi IP e dual-stack. IPv6

Indcirizzi IP

Gli indirizzi IP a cui vuoi che i resolver DNS sulla rete inoltrino le query DNS. Richiediamo di specificare un minimo di due indirizzi IP per la ridondanza. Tieni presente quanto segue:

Zone di disponibilità multiple

Consigliamo di specificare indirizzi IP in almeno due zone di disponibilità. È anche possibile specificare facoltativamente ulteriori indirizzi IP in quelle o in altre zone di disponibilità.

Indirizzi IP e interfacce di rete elastiche di Amazon VPC

Per ogni combinazione di zona di disponibilità, sottorete e indirizzo IP specificata, Resolver crea un'interfaccia di rete elastica di Amazon VPC. Per quanto riguarda il numero massimo di query DNS al secondo per ogni indirizzo IP in un endpoint, consulta Quote relative a Route 53 Resolver. Per informazioni sui prezzi per ogni interfaccia di rete elastica, consulta "Amazon Route 53" nella Pagina dei prezzi di Amazon Route 53.

> **Note**
>
> L'endpoint del risolutore ha un indirizzo IP privato. Questi indirizzi IP non cambieranno nel corso della vita di un endpoint.

Per ogni indirizzo IP, specifica i seguenti valori. Ogni indirizzo IP deve trovarsi in una zona di disponibilità del VPC specificato in VPC in the region-name Region (VPC nella regione region-name).

Zona di disponibilità

La zona di disponibilità nella quale desideri che le query DNS passino in direzione del VPC. La zona di disponibilità specificata deve essere configurata con una sottorete.

Sottorete

La sottorete che contiene gli indirizzi IP che desiderate assegnare al vostro endpoint Resolver. ENIs Questi sono gli indirizzi a cui invierai le query DNS. La sottorete deve avere a disposizione un indirizzo IP.

L'indirizzo IP della sottorete deve corrispondere al Tipo di endpoint.

Indirizzo IP

L'indirizzo IP al quale desideri inoltrare le query DNS.

Scegli se vuoi che sia Resolver a scegliere un indirizzo IP per tuo conto tra gli indirizzi IP disponibili nella sottorete specificata o se vuoi specificare personalmente l'indirizzo IP.

Se scegli di specificare tu stesso l'indirizzo IP, inserisci un IPv6 indirizzo IPv4 or o entrambi.

Protocolli

Il protocollo dell'endpoint determina il modo in cui i dati vengono trasmessi all'endpoint in entrata. Scegli uno o più protocolli, a seconda del livello di sicurezza necessario.

- Do53: (impostazione predefinita) i dati vengono inoltrati utilizzando Route 53 Resolver senza crittografia aggiuntiva. Sebbene i dati non possano essere letti da soggetti esterni, è possibile visualizzarli all'interno delle reti AWS .
- DoH: i dati vengono trasmessi attraverso una sessione HTTPS crittografata. DoH aggiunge un ulteriore livello di sicurezza in cui i dati non possono essere decrittografati da utenti non autorizzati né letti da nessuno all'infuori del destinatario previsto.
- DoH-FIPS: i dati vengono trasmessi attraverso una sessione HTTPS crittografata conforme allo standard di crittografia FIPS 140-2. Supportato solo per gli endpoint in entrata. Per ulteriori informazioni, consulta FIPS PUB 140-2.

> **Note**
>
> Per gli endpoint in entrata DOH/DOH-FIPS, esiste un problema noto a causa della pubblicazione di un IP di origine errato nella registrazione delle query di Route 53 Resolver.

Per un endpoint in entrata, è possibile applicare i protocolli come segue:

- Do53 e DoH in combinazione.
- Do53 e DoH-FIPS in combinazione.
- Do53 da solo.
- DoH da solo.
- DoH-FIPS da solo.
- Nessuno, il che equivale a Do53.

> **Important**
>
> Non è possibile modificare il protocollo di un endpoint in entrata direttamente dal solo Do53 al solo DoH o DoH-FIPS. Ciò serve a prevenire un'interruzione improvvisa del traffico in entrata basato su Do53. Per modificare il protocollo da Do53 a DoH o DoH-FIPS, devi innanzitutto abilitare sia Do53 che DoH oppure Do53 e DoH-FIPS, per garantire che tutto il traffico in entrata sia passato all'uso del protocollo DoH o DoH-FIPS, e quindi rimuovere il protocollo Do53.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Inoltro di query DNS in uscita alla rete

Per inoltrare alla tua rete le query DNS che provengono da EC2 istanze Amazon in una o più VPCs istanze, crei un endpoint in uscita e una o più regole:

Endpoint in uscita

Per inoltrare le query DNS dalla tua rete VPCs alla tua rete, crei un endpoint in uscita. Un endpoint in uscita specifica gli indirizzi IP da cui provengono le query. Tali indirizzi IP, che scegli dall'intervallo di indirizzi IP disponibili per il VPC, non sono indirizzi IP pubblici. Ciò significa che, per ogni endpoint in uscita, è necessario connettere il VPC alla rete mediante una connessione AWS Direct Connect , una connessione VPC o un gateway NAT (Network Address Translation). Tieni presente che puoi utilizzare lo stesso endpoint in uscita per più endpoint VPCs nella stessa regione oppure puoi creare più endpoint in uscita. Se desideri utilizzare il tuo endpoint in uscita

DNS64, puoi abilitare DNS64 l'utilizzo di Amazon Virtual Private Cloud. Per ulteriori informazioni, consulta DNS64 e NAT64 consulta la Amazon VPC User Guide.

L'IP di destinazione in base alla regola Route 53 Resolver viene scelto a caso da Resolver e non vi è alcuna preferenza nella scelta di un particolare IP di destinazione rispetto all'altro. Se un IP di destinazione non risponde alla richiesta DNS inoltrata, il Resolver riproverà a inserire un indirizzo IP casuale tra i destinatari. IPs

Assicurati che tutti gli indirizzi IP di destinazione siano raggiungibili dagli endpoint Resolver. Se Resolver non è in grado di inoltrare le query DNS in uscita a nessuno degli IP di destinazione, ciò può portare a tempi di risoluzione DNS prolungati.

Regolamento

Per specificare i nomi di dominio delle query che desideri inoltrare ai resolver DNS sulla rete, è necessario creare una o più regole. Ogni regola specifica un nome di dominio. Quindi associ le regole alle quali desideri inoltrare VPCs le query alla tua rete.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

Configurazione dell'inoltro in uscita

Per configurare Resolver in modo che inoltri query DNS che hanno origine nel VPC alla rete, procedi nel seguente modo.

> **Important**
>
> Dopo aver creato un endpoint in uscita, è necessario creare una o più regole e associarle a una o più. VPCs Le regole specificano i nomi di dominio delle query DNS che desideri inoltrare alla rete.

Per creare un endpoint in uscita

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, seleziona Outbound endpoints (Endpoint in uscita).

3. Nella barra di navigazione, seleziona la regione dove si desidera creare l'endpoint in uscita.
4. Scegli Create outbound endpoint (Crea endpoint in uscita).
5. Immetti i valori applicabili. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica degli endpoint in uscita.
6. Scegli Create (Crea) .

> **Note**
>
> La creazione di un endpoint in uscita richiede un paio di minuti. Non è possibile creare un altro endpoint in uscita fino a quando non viene creato il primo.

7. Creare una o più regole per specificare i nomi di dominio delle query DNS che si desidera inoltrare ai resolver DNS sulla rete. Per ulteriori informazioni, consulta la procedura successiva.

Per creare una o più regole di inoltro, procedere nel seguente modo.

Per creare regole di inoltro e associarle a una o più regole VPCs

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Rules (Regole).
3. Nella barra di navigazione, scegli la regione dove hai creato la regola.
4. Scegli Create rule (Crea regola).
5. Immetti i valori applicabili. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica delle regole.
6. Seleziona Save (Salva.
7. Per aggiungere un'altra regola, ripetere le fasi da 4 a 6.

Valori specificati durante la creazione o la modifica degli endpoint in uscita

Quando crei o modifichi un endpoint in uscita, devi specificare i seguenti valori:

ID Outpost

Se stai creando l'endpoint per un Resolver su un AWS Outposts VPC, questo è l'ID. AWS Outposts

Nome endpoint

Un nome descrittivo che ti consenta di trovare facilmente un endpoint in uscita.

VPC nella regione region-name.

Tutte le query DNS in uscita passeranno attraverso questo VPC in direzione della rete.

Gruppo di sicurezza per questo endpoint

L'ID di uno o più gruppi di sicurezza che si desidera utilizzare per controllare l'accesso a questo VPC. Il gruppo di sicurezza specificato deve includere una o più regole in uscita. Le regole in uscita devono consentire l'accesso TCP e UDP sulla porta che si sta utilizzando per le query DNS nella rete. Non è possibile modificare questo valore dopo avere creato un endpoint.

Alcune regole del gruppo di sicurezza consentiranno il tracciamento della connessione e potrebbero influire sul numero massimo di query al secondo dall'endpoint in uscita al nameserver di destinazione. Per evitare il tracciamento delle connessioni causato da un gruppo di sicurezza, vedi Connessioni non tracciate.

Per ulteriori informazioni, consultare Gruppi di sicurezza per il VPC nella Guida per l'utente di Amazon VPC.

Tipo di endpoint

Il tipo di endpoint può essere uno o due indirizzi IP IPv4 o IPv6 dual-stack. Per un endpoint dual-stack, l'endpoint avrà entrambi gli IPv6 indirizzi a cui il resolver DNS sulla rete IPv4 può inoltrare la query DNS.

> **Note**
>
> Per motivi di sicurezza, stiamo negando l'accesso diretto al IPv6 traffico Internet pubblico per tutti gli indirizzi IP e dual-stack. IPv6

Indirizzi IP

Gli indirizzi IP nel VPC ai quali desideri che Resolver inoltri le query DNS in direzione dei resolver sulla rete. Questi non sono gli indirizzi IP dei resolver DNS sulla rete; gli indirizzi IP dei resolver vengono specificati quando si creano le regole che si associano a una o più regole. VPCs Richiediamo di specificare un minimo di due indirizzi IP per la ridondanza.

> **Note**
>
> L'endpoint del risolutore ha un indirizzo IP privato. Questi indirizzi IP non cambieranno nel corso della vita di un endpoint.

Tieni presente quanto segue:

Zone di disponibilità multiple

Consigliamo di specificare indirizzi IP in almeno due zone di disponibilità. È anche possibile specificare facoltativamente ulteriori indirizzi IP in quelle o in altre zone di disponibilità.

Indirizzi IP e interfacce di rete elastiche di Amazon VPC

Per ogni combinazione di zona di disponibilità, sottorete e indirizzo IP specificata, Resolver crea un'interfaccia di rete elastica di Amazon VPC. Per quanto riguarda il numero massimo di query DNS al secondo per ogni indirizzo IP in un endpoint, consulta Quote relative a Route 53 Resolver. Per informazioni sui prezzi per ogni interfaccia di rete elastica, consulta "Amazon Route 53" nella Pagina dei prezzi di Amazon Route 53.

Ordine degli indirizzi IP

È possibile specificare gli indirizzi IP in qualsiasi ordine. Quando si inoltrano le query DNS, Resolver non sceglie gli indirizzi IP in base all'ordine in cui sono elencati.

Per ogni indirizzo IP, specifica i seguenti valori. Ogni indirizzo IP deve trovarsi in una zona di disponibilità del VPC specificato in VPC in the region-name Region (VPC nella regione region-name).

Zona di disponibilità

La zona di disponibilità nella quale desideri che le query DNS passino in direzione della rete. La zona di disponibilità specificata deve essere configurata con una sottorete.

Sottorete

La sottorete contenente l'indirizzo IP dal quale desideri provengano le query DNS verso la rete. La sottorete deve avere a disposizione un indirizzo IP.

L'indirizzo IP della sottorete deve corrispondere al Tipo di endpoint.

Indirizzo IP

L'indirizzo IP dal quale desideri provengano le query DNS verso la rete.

Scegli se vuoi che sia Resolver a scegliere un indirizzo IP per tuo conto tra gli indirizzi IP disponibili nella sottorete specificata o se vuoi specificare personalmente l'indirizzo IP.

Se scegli di specificare tu stesso l'indirizzo IP, inserisci un IPv4 indirizzo o entrambi. IPv6

Protocolli

Il protocollo dell'endpoint determina il modo in cui i dati vengono trasmessi dall'endpoint in uscita. Scegli uno o più protocolli, a seconda del livello di sicurezza necessario.

- Do53: (impostazione predefinita) i dati vengono inoltrati utilizzando Route 53 Resolver senza crittografia aggiuntiva. Sebbene i dati non possano essere letti da soggetti esterni, è possibile visualizzarli all'interno delle reti AWS .
- DoH: i dati vengono trasmessi attraverso una sessione HTTPS crittografata. DoH aggiunge un ulteriore livello di sicurezza in cui i dati non possono essere decrittografati da utenti non autorizzati né letti da nessuno all'infuori del destinatario previsto.

Per un endpoint in uscita è possibile applicare i protocolli come segue:

- Do53 e DoH in combinazione.
- Do53 da solo.
- DoH da solo.
- Nessuno, il che equivale a Do53.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Valori specificati durante la creazione o la modifica delle regole

Quando crei o modifichi una regola di inoltro, devi specificare i seguenti valori:

Nome regola

Un nome descrittivo che ti consenta di trovare facilmente una regola nel pannello di controllo.

Tipo di regola

Scegli il valore applicabile:

- Inoltra: scegli questa opzione se desideri inoltrare query DNS per un nome di dominio specifico ai resolver sulla rete.

- Sistema: scegli questa opzione se desideri che Resolver sostituisca il comportamento definito in una regola di inoltro. Quando crei una regola di sistema, Resolver risolve le query DNS per sottodomini specificati che altrimenti verrebbero risolti dai resolver DNS sulla rete.

Per impostazione predefinita, le regole di inoltro valgono per un nome di dominio e per tutti i relativi sottodomini. Se vuoi inoltrare le query per un dominio a un resolver sulla rete ma non vuoi inoltrare query per alcuni sottodomini, devi creare una regola di sistema per i sottodomini. Ad esempio, se crei una regola di inoltro per esempio.com ma non vuoi inoltrare query per acme.esempio.com, devi creare una regola di sistema e specificare acme.esempio.com come nome di dominio.

VPCs che usano questa regola

VPCs Che utilizzano questa regola per inoltrare le query DNS per il nome o i nomi di dominio specificati. Puoi applicare una regola a VPCs quante ne vuoi.

Nome dominio

Le query DNS per questo nome dominio vengono inoltrate agli indirizzi IP specificati in Indirizzi IP target. Per ulteriori informazioni, consulta Come Resolver determina se il nome di dominio in una query corrisponde alle regole.

Endpoint in uscita

Resolver inoltra le query DNS tramite l'endpoint in uscita qui specificato agli indirizzi IP specificati in Indirizzi IP di destinazione.

Indirizzi IP target

Quando una query DNS corrisponde al nome specificato in Domain name (Nome dominio), l'endpoint in uscita inoltra la query agli indirizzi IP che specifichi qui. In genere questi sono gli indirizzi IP dei resolver DNS sulla rete.

Target IP addresses (Indirizzi IP target) è disponibile solo quando il valore di Rule type (Tipo regola) è Forward (Inoltro).

IPv4 Specificate IPv6 gli indirizzi, i protocolli e che ServerNameIndication desiderate utilizzare per l'endpoint. ServerNameIndication è applicabile solo quando il protocollo selezionato è DoH.

La risoluzione dell'indirizzo IP di destinazione del nome di dominio completo di un resolver DoH sulla rete tramite l'endpoint in uscita non è supportata. Gli endpoint in uscita richiedono l'indirizzo IP di destinazione del resolver DoH sulla rete a cui inoltrare le query DoH. Se il resolver DoH

sulla rete richiede l'FQDN nell'SNI TLS e nell'intestazione HTTP Host, deve essere fornito. ServerNameIndication

ServerNameIndication

L'indicazione del nome del server DoH a cui si desidera inoltrare le interrogazioni. Viene utilizzata solo se il protocollo è DoH.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS bolletta. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella AWS Billing Guida per l'utente.

Gestione degli endpoint in entrata

Per gestire gli endpoint in entrata, esegui la procedura applicabile.

Argomenti

- Visualizzazione e modifica degli endpoint in entrata
- Visualizzazione dello stato degli endpoint in entrata
- Eliminazione degli endpoint in entrata

Visualizzazione e modifica degli endpoint in entrata

Per visualizzare e modificare le impostazioni di un endpoint in entrata, procedi nel seguente modo.

Per visualizzare e modificare le impostazioni di un endpoint in entrata.

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Inbound endpoints (Inbound in entrata).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in entrata.
4. Scegliere l'opzione per l'endpoint di cui si desidera visualizzare o modificare le impostazioni.
5. Scegliere View details (Visualizza dettagli) o Edit (Modifica).

Per informazioni sui valori per gli endpoint in entrata, consulta Valori specificati durante la creazione o la modifica di endpoint in entrata.

6. Se si sceglie Edit (Modifica), immettere i valori applicabili e selezionare Save (Salva).

Visualizzazione dello stato degli endpoint in entrata

Per visualizzare lo stato di un endpoint in entrata, eseguire la procedura seguente.

Per visualizzare lo stato di un endpoint in entrata

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Inbound endpoints (Inbound in entrata).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in entrata. La colonna Status (Stato) contiene uno dei seguenti valori:

   Creazione

   Resolver crea e configura una o più interfacce di rete di Amazon VPC per questo endpoint.

   Operational

   Le interfacce di rete di Amazon VPC per questo endpoint sono configurate correttamente e in grado di inoltrare il traffico in entrata e in uscita delle query DNS tra la rete e Resolver.

   Aggiornamento in corso

   Il resolver associa o annulla l'associazione di una o più interfacce di rete a questo endpoint.

   Auto recovering

   Resolver prova a ripristinare una o più interfacce di rete associate a questo endpoint. Durante il processo di ripristino, l'endpoint funziona con capacità limitata a causa del limite del numero di query DNS per indirizzo IP (per interfaccia di rete). Per il limite corrente, consulta Quote relative a Route 53 Resolver.

   Action needed

   Questo endpoint non è integro e Resolver non è in grado di ripristinarlo automaticamente. Per risolvere il problema, si consiglia di verificare ciascun indirizzo IP associato all'endpoint. Per ogni indirizzo IP non disponibile, aggiungere un altro indirizzo IP e quindi eliminare l'indirizzo

IP non disponibile. (Un endpoint deve sempre includere almeno due indirizzi IP). Un stato di Action needed (Operazione necessaria) può avere una serie di cause. Di seguito sono illustrate due cause comuni:

- Una o più interfacce di rete associate con l'endpoint sono state eliminate tramite Amazon VPC.
- Non è stato possibile creare l'interfaccia di rete per motivi al di fuori del controllo di Resolver.

Eliminazione in corso

Il resolver sta eliminando questo endpoint e le interfacce di rete associate.

Eliminazione degli endpoint in entrata

Per eliminare un endpoint in entrata, procedi nel seguente modo.

> **Important**
>
> Se elimini un endpoint in entrata, le query DNS dalla rete non vengono più inoltrare a Resolver nel VPC specificato nell'endpoint.

Per eliminare un endpoint in entrata

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Inbound endpoints (Inbound in entrata).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in entrata.
4. Selezionare l'opzione per l'endpoint che si desidera eliminare.
5. Scegli Elimina.
6. Per confermare che si desidera eliminare l'endpoint, immettere il nome dell'endpoint e scegliere Submit (Invia).

Gestione degli endpoint in uscita

Per gestire gli endpoint in uscita, esegui la procedura applicabile.

Argomenti

Visualizzazione e modifica degli endpoint in uscita

Per visualizzare e modificare le impostazioni di un endpoint in uscita, procedi nel seguente modo.

Per visualizzare e modificare le impostazioni di un endpoint in uscita.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Outbound endpoints (Endpoint in uscita).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in uscita.
4. Scegliere l'opzione per l'endpoint di cui si desidera visualizzare o modificare le impostazioni.
5. Scegliere View details (Visualizza dettagli) o Edit (Modifica).

   Per informazioni sui valori per gli endpoint in uscita, consulta Valori specificati durante la creazione o la modifica degli endpoint in uscita.
6. Se si sceglie Edit (Modifica), immettere i valori applicabili, quindi selezionare Save (Salva).

Visualizzazione dello stato degli endpoint in uscita

Per visualizzare lo stato di un endpoint in uscita, eseguire la procedura seguente.

Per visualizzare lo stato di un endpoint in uscita

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Outbound endpoints (Endpoint in uscita).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in uscita. La colonna Status (Stato) contiene uno dei seguenti valori:

Creazione

Resolver crea e configura una o più interfacce di rete di Amazon VPC per questo endpoint.

Operational

Le interfacce di rete di Amazon VPC per questo endpoint sono configurate correttamente e in grado di inoltrare il traffico in entrata e in uscita delle query DNS tra la rete e Resolver.

Aggiornamento in corso

Il resolver associa o annulla l'associazione di una o più interfacce di rete a questo endpoint.

Auto recovering

Resolver prova a ripristinare una o più interfacce di rete associate a questo endpoint. Durante il processo di ripristino, l'endpoint funziona con capacità limitata a causa del limite del numero di query DNS per indirizzo IP (per interfaccia di rete). Per il limite corrente, consulta Quote relative a Route 53 Resolver.

Action needed

Questo endpoint non è integro e Resolver non è in grado di ripristinarlo automaticamente. Per risolvere il problema, si consiglia di verificare ciascun indirizzo IP associato all'endpoint. Per ogni indirizzo IP non disponibile, aggiungere un altro indirizzo IP e quindi eliminare l'indirizzo IP non disponibile. (Un endpoint deve sempre includere almeno due indirizzi IP). Un stato di Action needed (Operazione necessaria) può avere una serie di cause. Di seguito sono illustrate due cause comuni:

- Una o più interfacce di rete associate con l'endpoint sono state eliminate tramite Amazon VPC.
- Non è stato possibile creare l'interfaccia di rete per motivi al di fuori del controllo di Resolver.

Eliminazione in corso

Il resolver sta eliminando questo endpoint e le interfacce di rete associate.

Eliminazione degli endpoint in uscita

Prima di poter eliminare un endpoint, devi prima eliminare tutte le regole associate a un VPC.

Per eliminare un endpoint in uscita, procedi nel seguente modo.

> **Important**
>
> Se elimini un endpoint in uscita, Resolver smette di inoltrare query DNS dal tuo VPC alla rete per le regole che specificano l'endpoint in uscita eliminato.

Per eliminare un endpoint in uscita

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Outbound endpoints (Endpoint in uscita).
3. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint in uscita.
4. Selezionare l'opzione per l'endpoint che si desidera eliminare.
5. Scegli Elimina.
6. Per confermare che si desidera eliminare l'endpoint, immettere il nome dell'endpoint, quindi scegliere Submit (Invia).

Gestione delle regole di inoltro

Se vuoi che Resolver inoltri query per nomi di dominio specifici alla rete, devi creare una regola di inoltro per ciascun nome di dominio e specificare il nome del dominio per cui desideri inoltrare le query.

Argomenti

Visualizzazione e modifica delle regole di inoltro

Per visualizzare e modificare le impostazioni di una regola di inoltro, procedi nel seguente modo.

Per visualizzare e modificare le impostazioni di una regola di inoltro

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Regole.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.
4. Scegliere l'opzione per la regola di cui si desidera visualizzare o modificare le impostazioni.
5. Scegliere View details (Visualizza dettagli) o Edit (Modifica).

   Per informazioni sui valori per le regole di inoltro, consulta Valori specificati durante la creazione o la modifica delle regole.
6. Se si sceglie Edit (Modifica), immettere i valori applicabili, quindi selezionare Save (Salva).

Creazione delle regole di inoltro

Per creare una o più regole di inoltro, procedere nel seguente modo.

Per creare regole di inoltro e associarle a una o più regole VPCs

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Rules (Regole).
3. Nella barra di navigazione, scegli la regione dove hai creato la regola.
4. Scegli Create rule (Crea regola).
5. Immetti i valori applicabili. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica delle regole.
6. Seleziona Save (Salva.
7. Per aggiungere un'altra regola, ripetere le fasi da 4 a 6.

Aggiunta di regole per la ricerca inversa

Se è necessario controllare le ricerche inverse nel VPC, è possibile aggiungere regole all'endpoint del resolver in uscita.

Come creare la regola di ricerca inversa

1. Segui le fasi descritte nella procedura precedente, fino alla fase 5.
2. Quando specifichi la regola, specifica il record PTR per l'indirizzo o gli indirizzi IP per i quali desideri una regola di inoltro di ricerca inversa.

   Ad esempio, se è necessario inoltrare ricerche per indirizzi nell'intervallo 10.0.0.0/23, specifica due regole:

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

   Qualsiasi indirizzo IP in tali sottoreti verrà considerato come sottodominio di tali registri PTR. Ad esempio, 10.0.1.161 avrà un indirizzo di ricerca inversa 161.1.0.10.in-addr.apra, che è un sottodominio di 1.0.10.in-addra.apra.
3. Specifica il server a cui inoltrare queste ricerche.
4. Aggiungi queste regole all'endpoint del resolver in uscita.

Tieni presente che l'attivazione di `enableDNSHostNames` per il VPC aggiunge automaticamente i record PTR. Per informazioni, consulta Che cos'è Amazon Route 53 Resolver?. La procedura precedente è necessaria solo se si desidera specificare esplicitamente un resolver per determinati intervalli IP, ad esempio quando si inoltrano query a un server Active Directory.

Associazione di regole di inoltro a un VPC

Dopo aver creato una regola di inoltro, devi associarla a una o più regole. VPCs Le regole saranno valide solo dopo essere state associate a un VPC. Quando associ una regola a un VPC, Resolver inizia a inoltrare le query DNS per il nome di dominio specificato nella regola ai resolver DNS specificati nella regola. Le query passano per l'endpoint in uscita specificato al momento della creazione della regola.

Per associare una regola di inoltro a una o più VPCs

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Regole.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.
4. Scegli il nome della regola che desideri associare a una o più regole VPCs.
5. Scegli Associa VPC.
6. In base VPCs a questa regola, scegli la regola a VPCs cui desideri associare la regola.
7. Scegli Aggiungi.

Rimozione dell'associazione di regole di inoltro da un VPC

Viene rimossa l'associazione di una regola di inoltro da un VPC nei seguenti casi:

- Per le query DNS che hanno origine in questo VPC, desideri che Resolver smetta di inoltrare query per il nome di dominio specificato nella regola alla rete.
- Vuoi eliminare la regola di inoltro. Se una regola è attualmente associata a una o più regole VPCs, è necessario dissociarla da tutte le regole VPCs prima di poterla eliminare.

Se si desidera dissociare una regola di inoltro da una o più regole VPCs, eseguire la procedura seguente.

Per rimuovere l'associazione di una regola di inoltro da un VPC

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Regole.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.
4. Scegli il nome della regola da cui desideri dissociare da una o più VPCs regole.
5. Scegliere l'opzione per il VPC da cui si desidera annullare l'associazione della regola.
6. Scegli Dissocia.
7. Digitare disassociate (annulla associazione) per confermare.
8. Scegli Invia.

Condivisione delle regole del Resolver con altri AWS account e utilizzo di regole condivise

Puoi condividere le regole Resolver che hai creato utilizzando un AWS account con altri account. AWS Per condividere le regole, la console Route 53 Resolver si integra con AWS Resource Access Manager. Per ulteriori informazioni su Resource Access Manager, consulta la Guida per l'utente a Resource Access Manager.

Tieni presente quanto segue:

Associazione di regole condivise con VPCs

Se un altro AWS account ha condiviso una o più regole con il tuo account, puoi associare le regole VPCs allo stesso modo in cui associ le regole che hai creato al tuo VPCs. Per ulteriori informazioni, consulta Associazione di regole di inoltro a un VPC.

Eliminazione di una regola o rimozione della condivisione

Se condividi una regola con altri account e poi elimini la regola o interrompi la condivisione e se la regola era associata a uno o più VPCs, Route 53 Resolver inizia a elaborare le query DNS per quelle VPCs basate sulle regole rimanenti. Il comportamento è la stesso di quando si rimuove l'associazione della regola dal VPC.

Se una regola viene condivisa con un'unità organizzativa (OU) e un account nell'unità organizzativa viene spostato in un'altra OU, tutte le associazioni con la regola condivisa a qualsiasi VPC nell'account verranno eliminate. Tuttavia, se la regola Resolver era già condivisa con l'unità organizzativa di destinazione, l'associazione VPC rimarrà intatta e non verrà dissociata.

Numero massimo di regole e associazioni

Quando un account crea una regola e la condivide con uno o più altri account, il numero massimo di regole per AWS regione si applica all'account che ha creato la regola.

Quando un account con cui è condivisa una regola associa la regola a uno o più VPCs, il numero massimo di associazioni tra le regole e VPCs per regione si applica all'account con cui la regola è condivisa.

Per le quote correnti di Resolver, consulta Quote relative a Route 53 Resolver.

Autorizzazioni

Per condividere una regola con un altro AWS account, devi disporre dell'autorizzazione per utilizzare l'PutResolverRulePolicyazione.

Restrizioni sull' AWS account con cui è condivisa una regola

L'account con cui si condivide una regola non può modificare né eliminare la regola.

Assegnazione di tag

Solo l'account che ha creato una regola può aggiungere, eliminare o visualizzare i tag della regola.

Per visualizzare lo stato di condivisione attuale di una regola (incluso l'account che ha condiviso la regola o l'account con cui la regola è condivisa) e per condividere regole con un altro account, procedi nel seguente modo.

Per visualizzare lo stato di condivisione e le regole di condivisione con un altro AWS account

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Regole.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.

   La colonna Sharing status (Stato condivisione) mostra l'attuale stato delle regole create dall'account attuale o condivise con l'account attuale.

   - Non condivisa: l' AWS account corrente ha creato la regola e la regola non è condivisa con altri account.
   - Condivisa da me: l'attuale account ha creato la regola e l'ha condivisa con uno o più account.
   - Condivisa con me: un altro account ha creato la regola e l'ha condivisa con l'account attuale.
4. Scegliere il nome della regola di cui si desidera visualizzare le informazioni di condivisione o che si desidera condividere con un altro account.

   Nella *rule name* pagina Regola:, il valore in Proprietario mostra l'ID dell'account che ha creato la regola. Questo è l'account attuale, a meno che il valore di Sharing status (Stato di condivisione) non sia Shared with me (Condivisa con me). In questo caso, il Owner (Proprietario) è l'account che ha creato la regola e l'ha condivisa con l'account attuale.
5. Selezionare Share (Condividi) per visualizzare ulteriori informazioni o per condividere la regola con un altro account. Viene visualizzata una pagina nella console Resource Access Manager, a seconda del valore di Sharing status (Stato di condivisione):

- Non condivisa: viene visualizzata la pagina Create resource share (Crea condivisione risorsa). Per ulteriori informazioni su come condividere la regola con un altro account, UO o organizzazione, passa alla fase 6.
- Condivisa da me: la pagina Shared resources (Risorse condivise) mostra le regole e le altre risorse di proprietà dell'account attuale e condivise con altri account.
- Condivisa con me: la pagina Shared resources (Risorse condivise) mostra le regole e le altre risorse di proprietà di altri account e condivise con l'account attuale.

6. Per condividere una regola con un altro AWS account, unità organizzativa o organizzazione, specifica i seguenti valori.

> **Note**
>
> Non è possibile aggiornare le impostazioni di condivisione. Se vuoi modificare una delle seguenti impostazioni, devi ricondividere una regola con le nuove impostazioni e rimuovere le precedenti impostazioni di condivisione.

Descrizione

Inserisci una breve descrizione che ti aiuta a ricordare perché hai condiviso la regola.

Risorse

Seleziona la casella di controllo per la regola che vuoi condividere.

Principali

Immettere il numero di AWS account, il nome dell'unità organizzativa o il nome dell'organizzazione.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS fattura; è possibile utilizzare anche i tag per altri scopi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Eliminazione delle regole di inoltro

Per eliminare una regola di inoltro, procedi nel seguente modo.

Tieni presente quanto segue:

- Se la regola di inoltro è associata a una regola VPCs, è necessario dissociarla dalla regola VPCs prima di poter eliminare la regola. Per ulteriori informazioni, consulta Rimozione dell'associazione di regole di inoltro da un VPC.
- Non è possibile eliminare la regola predefinita Internet Resolver che ha un valore Recursive (Ricorsivo) per Type (Tipo). Questa regola consente a Route 53 Resolver di funzionare come resolver ricorsivo per tutti i nomi di dominio per i quali non sono state create regole personalizzate e per i quali Resolver non ha creato regole autodefinite. Per ulteriori informazioni su come sono classificate le regole, consulta Utilizzo di regole per controllare quali query vengono inoltrate alla rete.

Per eliminare una regola di inoltro

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Regole.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.
4. Selezionare l'opzione per la regola che si desidera eliminare.
5. Scegli Elimina.
6. Per confermare che si desidera eliminare la regola, immettere il nome della regola e scegliere Submit (Invia).

Regole di inoltro per le query DNS inverse in Resolver

Quando `enableDnsHostnames` e `enableDnsSupport` sono impostati su `true` per un cloud privato virtuale (VPC) di Amazon VPC, Resolver crea automaticamente regole di sistema definite automaticamente per query DNS inverse. Per ulteriori informazioni su queste impostazioni, consulta Attributi DNS nel VPC nella Guida per gli sviluppatori di Amazon VPC.

Le regole di inoltro per le query DNS inverse sono particolarmente utili per servizi come SSH o Active Directory, che hanno la possibilità di autenticare gli utenti eseguendo una ricerca DNS inversa per

l'indirizzo IP da cui un cliente sta tentando di connettersi a una risorsa. Per ulteriori informazioni sulle regole di sistema definite automaticamente, consulta Nomi di dominio per cui Resolver crea regole di sistema autodefinite.

È possibile disattivare queste regole e modificare tutte le query DNS inverse in modo che vengano, ad esempio, inoltrate ai server dei nomi locali per la risoluzione.

Dopo aver disattivato le regole automatiche, crea regole per inoltrare le query secondo necessità alle risorse locali. Per ulteriori informazioni su come gestire le regole di inoltro, consulta Gestione delle regole di inoltro.

Per disattivare le regole definite automaticamente

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, in Resolver scegli VPCs, quindi scegli un ID VPC.
3. In Regole autodefinite per la risoluzione DNS inversa, deselezionare la casella di controllo. Se la casella di controllo è già deselezionata, è possibile selezionarla per attivare la risoluzione DNS inversa definita automaticamente.

Per informazioni correlate APIs, vedi Configurazione del Resolver. APIs

Abilitazione della convalida DNSSEC in Amazon Route 53

Quando abiliti la convalida DNSSEC per un Virtual Private Cloud (VPC) in Amazon Route 53 Resolver, le firme DNSSEC vengono controllate crittograficamente per garantire che la risposta non sia stata manomessa. È possibile abilitare la convalida DNSSEC nella pagina dei dettagli del VPC.

La convalida DNSSEC è applicata da Route 53 Resolver ai nomi pubblici con firma quando questo esegue una risoluzione DNS ricorsiva.

Tuttavia, se Route 53 Resolver effettua un inoltro a un altro resolver DNS, tale resolver eseguirà una risoluzione DNS ricorsiva e dovrà pertanto applicare anche la convalida DNSSEC.

Important

L'abilitazione della convalida DNSSEC può influire sulla risoluzione DNS per i record DNS pubblici dalle risorse AWS in un VPC, che potrebbe causare un'interruzione. L'attivazione o la disattivazione della convalida DNSSEC può richiedere alcuni minuti.

Note

Al momento, il Amazon Route 53 Resolver bit di intestazione EDNS del VPC (noto anche come AmazonProvided DNS) ignora il bit di intestazione EDNS DO (DNSSEC OK) e il bit CD (Checking Disabled) nella query DNS. Se hai configurato DNSSEC, significa che sebbene il risolutore Route 53 esegua la convalida DNSSEC, non restituisce i record DNSSEC né imposta il bit AD nella risposta. Pertanto, l'esecuzione della convalida DNSSEC personalizzata non è attualmente supportata dal risolutore Route 53. Se ne hai bisogno, dovrai eseguire la tua risoluzione DNS ricorsiva.

Come abilitare la convalida DNSSEC per un VPC

1. Accedi e apri la console Route 53 all'indirizzo. AWS Management Console https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, sotto Resolver, scegli. VPCs
3. In Convalida DNSSEC, seleziona la casella di controllo. Se la casella di controllo è già selezionata, puoi deselezionarla e disabilitare la convalida DNSSEC.

   L'attivazione o la disattivazione della convalida DNSSEC può richiedere alcuni minuti.

Instradamento del traffico Internet verso le tue risorse AWS

Puoi utilizzare Amazon Route 53 per indirizzare il traffico verso una varietà di AWS risorse.

- Routing del traffico a un'API di Amazon API Gateway usando il proprio nome di dominio
- Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio
- Instradamento del traffico verso un'istanza Amazon EC2
- Instradamento del traffico verso un servizio AWS App Runner
- Instradamento del traffico verso un ambiente AWS Elastic Beanstalk
- Routing del traffico a un load balancer ELB
- Routing del traffico a un sito Web ospitato in un bucket Amazon S3
- Routing del traffico a un endpoint di interfaccia di Amazon Virtual Private Cloud usando il proprio nome dominio
- Instradamento del traffico verso Amazon WorkMail
- Instradamento del traffico verso l'endpoint OpenSearch del dominio Amazon Service
- Indirizzamento del traffico verso altre risorse AWS
- Creazione di Amazon Route 53 e Amazon Route 53 Resolver risorse con AWS CloudFormation

Routing del traffico a un'API di Amazon API Gateway usando il proprio nome di dominio

Puoi utilizzare Amazon API Gateway per creare, pubblicare, gestire, monitorare e proteggere APIs. Puoi creare APIs tali AWS servizi di accesso o altri servizi Web oltre ai dati archiviati nel AWS cloud.

Il metodo utilizzato per instradare il traffico di dominio a un'API di API Gateway è lo stesso indipendentemente dal fatto che sia stato creato un endpoint API Gateway regionale o un endpoint API Gateway ottimizzato per l'edge. Se crei un endpoint API Gateway privato, il processo è leggermente diverso.

- Endpoint API regionale: viene creato un record alias Route 53 che instrada il traffico all'endpoint API regionale.

- Endpoint API ottimizzato per l'edge: è possibile creare un record alias Route 53 che indirizza il traffico all'API ottimizzata per l'edge. Ciò fa sì che il traffico venga indirizzato alla CloudFront distribuzione associata all'API ottimizzata per i dispositivi perimetrali.
- Endpoint API privato: crei un record di alias Route 53 che indirizza il traffico verso il tuo endpoint API privato utilizzando un endpoint VPC di interfaccia per API Gateway in una zona ospitata privata.

Un record alias è un'estensione di Route 53 al DNS simile a un record CNAME. Per un confronto tra alias e record CNAME, consulta Scelta tra record alias e non alias.

> **Note**
>
> Route 53 non addebita alcun costo per le query di alias su API Gateway APIs o altre AWS risorse.

Argomenti

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

- Un'API di API Gateway che dispone di un nome di dominio personalizzato, ad esempio api.example.com, che corrisponde al nome del record Route 53 che desideri creare.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  - Configurazione di nomi di dominio personalizzati per HTTP APIs nell'Amazon API Gateway Developer Guide.
  - Configurazione di nomi di dominio personalizzati per REST APIs nell'Amazon API Gateway Developer Guide.
  - Configurazione di nomi di dominio personalizzati per WebSocket APIs l'Amazon API Gateway Developer Guide.
  - Nomi di dominio personalizzati per uso privato APIs in API Gateway nella Amazon API Gateway Developer Guide.

- Un nome di dominio registrato. Puoi utilizzare Amazon Route 53 come registrar di dominio oppure utilizzare un altro registrar.
- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Configurazione di Route 53 per instradare il traffico a un endpoint API Gateway

Per configurare Route 53 per instradare il traffico a un endpoint di API Gateway, completa la seguente procedura.

Custom domain names for public APIs

La procedura seguente descrive come indirizzare il traffico verso un endpoint API Gateway per un nome di dominio personalizzato per il pubblico APIs.

Come instradare il traffico a un endpoint di API Gateway

1. Se la zona ospitata Route 53 e l'endpoint sono stati creati utilizzando lo stesso account, passa alla fase 2.

   Se la zona ospitata e l'endpoint sono stati creati utilizzando account diversi, recupera il nome di dominio di destinazione per il nome di dominio personalizzato che desideri utilizzare:

   a. Accedi AWS Management Console e apri la console API Gateway all'indirizzo https://console.aws.amazon.com/apigateway/.
   b. Nel pannello di navigazione, scegli Nomi di dominio personalizzati.
   c. Seleziona il nome di dominio personalizzato che desideri utilizzare e recupera il valore di Nome dominio di API Gateway.
2. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Scegli il nome della zona ospitata che ha il nome di dominio che desideri utilizzare per instradare il traffico verso l'API.
5. Scegli Crea record.

6. Specifica i seguenti valori:

> **Important**
>
> Ti consigliamo di attivare Alias. Per i nomi di dominio che non utilizzano un record di alias Route 53, potresti riscontrare problemi se utilizzi un VPC con DNS privato abilitato a richiamare un'API privata. Il DNS privato sostituisce il comportamento di risoluzione DNS predefinito all'interno del VPC, il che potrebbe causare conflitti con i record DNS esterni.

Policy di routing

Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

Nome record

Immettere il nome di dominio da utilizzare per instradare il traffico verso l'API.

L'API verso cui instradare il traffico deve includere un nome di dominio personalizzato, ad esempio api.example.com, che corrisponde al nome del record Route 53.

Alias

Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

Valore/instradamento traffico a

Scegli Alias per l'API di API Gateway, quindi scegli la regione da cui proviene l'endpoint.

Il modo in cui si specifica il valore per Endpoint dipende dal fatto che la zona ospitata e l'API siano state create utilizzando lo stesso account o account diversi: AWS

- Stesso account: l'elenco dei nomi di dominio di destinazione include solo APIs quelli con un nome di dominio personalizzato che corrisponde al valore specificato per Record name. Scegli il valore applicabile.
- Account diversi: specifica il valore ottenuto nella fase 1 di questa procedura.

Tipo di record

Scegli A — IPv4 indirizzo.

Valutazione dello stato della destinazione

Per verificare il failover DNS, configura i controlli dell'integrità personalizzati. Per un esempio, consulta la sezione Configurare i controlli dell'integrità personalizzati per il failover DNS nella Guida per l'utente di API Gateway.

7. Scegli Crea record.

   In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarà possibile instradare il traffico all'istanza API; utilizzando il record alias creato in questa procedura.

Custom domain names for private APIs

La procedura seguente descrive come indirizzare il traffico verso un endpoint API Gateway per un nome di dominio personalizzato per uso privato APIs.

Come instradare il traffico a un endpoint di API Gateway

1. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome della zona ospitata privata con il nome di dominio che desideri utilizzare per indirizzare il traffico verso la tua API.
4. Scegli Crea record.
5. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Immettere il nome di dominio da utilizzare per instradare il traffico verso l'API.

   L'API verso cui instradare il traffico deve includere un nome di dominio personalizzato, ad esempio api.example.com, che corrisponde al nome del record Route 53.

   Alias

   Attiva Alias.

Valore/instradamento traffico a

Scegli Alias to VPC Endpoint. Scegli la regione da cui proviene l'endpoint, quindi seleziona il tuo endpoint VPC.

Tipo di record

Se lo utilizzi IPv6 per il tuo endpoint VPC, crea un tipo di record AAAA. Se utilizzi dualstack per il tuo endpoint VPC, crea un tipo di record sia AAAA che A.

Valutazione dello stato della destinazione

Per verificare il failover DNS, configura i controlli dell'integrità personalizzati. Per un esempio, consulta la sezione Configurare i controlli dell'integrità personalizzati per il failover DNS nella Guida per l'utente di API Gateway.

6. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarà possibile instradare il traffico all'istanza API; utilizzando il record alias creato in questa procedura.

Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio

Puoi usare Amazon CloudFront, la rete di distribuzione AWS dei contenuti (CDN), come un modo per velocizzare la distribuzione dei tuoi contenuti web. CloudFront è in grado di distribuire l'intero sito Web, inclusi contenuti dinamici, statici, in streaming e interattivi, utilizzando una rete globale di edge location. Gli utenti che richiedono i tuoi contenuti vengono instradati automaticamente alla posizione edge che offre loro la latenza minima.

> **Note**
>
> È possibile indirizzare il traffico verso una CloudFront distribuzione solo per le zone pubbliche ospitate.

Da utilizzare CloudFront per distribuire il contenuto del tuo sito Web, crea una distribuzione e specifica le relative impostazioni. Ad esempio, specifica il bucket Amazon S3 o il server HTTP da

cui desideri CloudFront ricevere i tuoi contenuti, se desideri che solo gli utenti selezionati abbiano accesso ai tuoi contenuti e se desideri che gli utenti utilizzino HTTPS.

Quando crei una distribuzione, CloudFront assegna un nome di dominio alla distribuzione, ad esempio d111111abcdef8.cloudfront.net. Puoi utilizzare questo nome di dominio URLs per i tuoi contenuti, ad esempio:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

In alternativa, puoi utilizzare il tuo nome di dominio in URLs, ad esempio:

```
http://example.com/logo.jpg
```

Segui i passaggi dell'Amazon CloudFront Developer Guide per utilizzare il tuo nome di dominio nei tuoi file URLs in una CloudFront distribuzione, anziché il nome di dominio CloudFront assegnato alla tua distribuzione. Per ulteriori informazioni sull'utilizzo del tuo nome di dominio con una CloudFront distribuzione, consulta Usare nomi di dominio personalizzati URLs aggiungendo nomi di dominio alternativi (). CNAMEs

Quando utilizzi un nome di dominio Route 53 con una CloudFront distribuzione, usa Amazon Route 53 per creare un record di alias che punti alla tua CloudFront distribuzione. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, ma è possibile creare un record alias sia per il dominio root, ad esempio esempio.com, sia per sottodomini, ad esempio www.esempio.com. (È possibile creare record CNAME solo per sottodomini). Quando Route 53 riceve una query DNS che corrisponde al nome e al tipo di un determinato record alias, Route 53 risponde con il nome dominio associato alla distribuzione.

> **Note**
>
> Route 53 non addebita alcun costo per le richieste di alias a CloudFront distribuzioni o altre risorse. AWS

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

1. Un nome di dominio registrato. Puoi utilizzare Amazon Route 53 come registrar di dominio oppure utilizzare un altro registrar.

2. Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

   Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

3. Richiedi un certificato pubblico in modo che CloudFront le distribuzioni Amazon richiedano HTTPS. Per ulteriori informazioni, consulta Fase 2: Richiesta di un certificato pubblico e Convalida DNS in AWS Certificate Manager nella Guida per l'utente di AWS Certificate Manager .

4. Una CloudFront distribuzione. La distribuzione deve includere un nome di dominio alternativo che corrisponda al nome di dominio che desideri utilizzare per la tua URLs anziché al nome di dominio CloudFront assegnato alla tua distribuzione.

   Ad esempio, se desideri che i URLs tuoi contenuti contengano il nome di dominio example.com, il campo Nome di dominio alternativo per la distribuzione deve includere example.com.

   Per ulteriori informazioni, consulta la seguente documentazione nell'Amazon CloudFront Developer Guide:

   - Procedura per la creazione di una distribuzione
   - Creazione o aggiornamento di una distribuzione tramite la console CloudFront

Configurazione di Amazon Route 53 per instradare il traffico verso una distribuzione CloudFront

Per configurare Amazon Route 53 per indirizzare il traffico verso una CloudFront distribuzione, segui questi passaggi. Per ulteriori informazioni sull'utilizzo del tuo nome di dominio con una CloudFront distribuzione, consulta Using custom URLs by adding alternate domain names (CNAMEs) nella Amazon CloudFront Developer Guide.

> **Note**
>
> In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Quando le modifiche si propagano, sarai in grado di indirizzare il traffico verso la tua CloudFront distribuzione utilizzando il nome del record di alias creato in questa procedura.

Per instradare il traffico in una distribuzione CloudFront

1. Ottieni il nome di dominio CloudFront assegnato alla tua distribuzione e determina se IPv6 è abilitato:

   a. Accedi a AWS Management Console e apri la CloudFront console all'indirizzohttps://console.aws.amazon.com/cloudfront/v4/home.

   b. Nella colonna ID seleziona il nome collegato della distribuzione a cui desideri instradare il traffico (non la casella di controllo).

   c. Nella scheda General (Generale), ottieni il valore del campo Distribution domain name (Nome del dominio di distribuzione).

   d. Nella scheda Generale, nella sezione Impostazioni, scegli modifica e scorri per controllare il IPv6campo per vedere se IPv6 è abilitato per la distribuzione. Se IPv6 è abilitato, dovrai creare due record di alias per la distribuzione, uno per instradare il IPv4 traffico verso la distribuzione e uno per instradare il IPv6 traffico. Seleziona Annulla.

      Per ulteriori informazioni, consulta Abilita IPv6 nell'argomento Valori che specifichi quando crei o aggiorni una distribuzione nell'Amazon CloudFront Developer Guide.

2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Scegli il nome collegato della zona ospitata per il dominio che desideri utilizzare per indirizzare il traffico verso la tua CloudFront distribuzione.
5. Scegli Crea record.

   Per creare i record puoi utilizzare la procedura guidata oppure puoi scegliere Switch to quick create (Passa alla creazione rapida).

6. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Inserisci il nome di dominio che desideri utilizzare per indirizzare il traffico verso la tua CloudFront distribuzione. Il valore predefinito è il nome della hosted zone.

Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico alla tua distribuzione, digita acme.

Alias

Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

> **Important**
>
> È necessario creare un record Alias affinché la CloudFront distribuzione funzioni.

Valore/instradamento traffico a

Scegli Alias per le distribuzioni. CloudFront La regione selezionata di default è us-east-1. Scegli il nome di dominio CloudFront assegnato alla distribuzione al momento della creazione. Questo è il valore ottenuto nella fase 1.

Tipo di record

Scegli A — IPv4 indirizzo.

Se IPv6 è abilitato per la distribuzione e stai creando un secondo record, scegli AAAA — IPv6 indirizzo.

Valutazione dello stato della destinazione

Accettare il valore predefinito No.

7. Scegli Crea record.
8. Se IPv6 è abilitato per la distribuzione, ripeti i passaggi da 5 a 7. Specifica le stesse impostazioni a eccezione del campo Tipo di record, come descritto nella fase 6.

Instradamento del traffico verso un'istanza Amazon EC2

Amazon EC2 offre capacità di elaborazione scalabile nel AWS cloud. Puoi avviare un ambiente di elaborazione EC2 virtuale (un'istanza) utilizzando un modello preconfigurato (Amazon Machine Image o AMI). All'avvio di un' EC2 istanza, installa EC2 automaticamente il sistema operativo (Linux o Microsoft Windows) e il software aggiuntivo incluso nell'AMI, come il software del server Web o del database.

Puoi indirizzare il traffico per il tuo dominio, ad esempio example.com, al tuo server utilizzando Amazon Route 53, se stai ospitando un sito Web o eseguendo un'applicazione Web su un' EC2 istanza.

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

- Un' EC2 istanza Amazon. Per informazioni sul lancio di un' EC2 istanza, consulta la seguente documentazione:
  - Linux: consulta la sezione Guida introduttiva alle istanze di Amazon EC2 Linux nella Amazon EC2 User Guide
  - Microsoft Windows: consulta la sezione Guida introduttiva alle istanze di Amazon EC2 Windows nella Amazon EC2 User Guide

  > **Important**
  >
  > Ti consigliamo anche di creare un indirizzo IP elastico e associarlo alla tua EC2 istanza. Un indirizzo IP elastico garantisce che l'indirizzo IP della tua EC2 istanza Amazon non venga mai modificato. Per informazioni relative ai prezzi, consulta Prezzi degli indirizzi IP elastici.

- Un nome di dominio registrato. Puoi utilizzare Amazon Route 53 come registrar di dominio oppure utilizzare un altro registrar.
- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Configurazione di Amazon Route 53 per instradare il traffico verso un'istanza Amazon EC2

Per configurare Amazon Route 53 per indirizzare il traffico verso un' EC2 istanza, esegui la seguente procedura.

Per indirizzare il traffico verso un' EC2 istanza Amazon

1. Ottieni l'indirizzo IP per l' EC2 istanza Amazon:

a. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.

b. Nell'elenco delle regioni nell'angolo in alto a destra della console, selezionare l'area in cui è stata avviata l'istanza.

c. Nel pannello di navigazione, seleziona Instances (Istanze).

d. Nella tabella, scegli l'istanza a cui desideri instradare il traffico.

e. Nel riquadro inferiore, nella scheda Descrizione, ottieni il valore di Elastic IPs.

   Se non hai associato un IP elastico all'istanza, puoi ottenere il valore di un IPv4 IP pubblico.

2. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Scegli il nome della zona ospitata corrisponde al nome del dominio che desideri utilizzare a cui instradare il traffico.
5. Scegli Crea record.
6. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Inserisci il nome di dominio che desideri utilizzare per indirizzare il traffico verso la tua EC2 istanza. Il valore predefinito è il nome della hosted zone.

   Ad esempio, se il nome della zona ospitata è example.com e desideri utilizzare acme.example.com per indirizzare il traffico verso la tua istanza, inserisci acme. EC2

   Valore/instradamento traffico a

   Scegli Indirizzo IP o altro valore a seconda del tipo di record. Digita l'indirizzo IP ottenuto nella fase 1.

   Tipo di record

   Scegli A — indirizzo. IPv4

TTL (secondi)

Accetta il valore di default di 300.

7. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarai in grado di indirizzare il traffico verso la tua EC2 istanza utilizzando il nome del record creato in questa procedura.

> **Important**
>
> Se rilasci l'IP elastico, assicurati di eliminare anche il record DNS che punta a questo. Se non lo fai, avrai un record DNS in sospeso che può essere rilevato da un utente non autorizzato.

Instradamento del traffico verso un servizio AWS App Runner

AWS App Runner è un servizio completamente gestito che consente agli sviluppatori di implementare facilmente applicazioni Web containerizzate e su larga scala e senza alcuna esperienza precedente APIs in materia di infrastruttura. Inizia con il tuo codice sorgente o un'immagine del container. App Runner crea e distribuisce l'applicazione Web automaticamente, bilancia il carico del traffico con la crittografia, si adatta alle tue esigenze di traffico e semplifica la comunicazione dei tuoi servizi con altri AWS servizi e applicazioni eseguiti in un Amazon VPC privato. Grazie ad App Runner, invece di pensare ai server o alla scalabilità, hai più tempo per concentrarti sulle tue applicazioni. Per ulteriori informazioni, consulta Che cos'è AWS App Runner? nella Guida per gli sviluppatori di AWS App Runner .

> **Important**
>
> Amazon Route 53 attualmente supporta i record di alias per AWS App Runner i servizi creati dopo il 1° agosto 2022.

Per instradare il traffico di dominio a un servizio App Runner, utilizza Amazon Route 53 per creare un record di alias che punti al servizio. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, tranne per il fatto che puoi creare un record alias sia per il dominio root, ad esempio

esempio.com, sia per i sottodomini, ad esempio www.esempio.com (http://www.esempio.com/). Puoi creare record CNAME solo per sottodomini.

> **Note**
>
> Route 53 non prevede costi per le query di alias rivolte al servizio App Runner o ad altre risorse AWS .

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

- Un servizio App Runner. Per informazioni sulla creazione di un servizio App Runner, consulta Guida introduttiva ad App Runner.
- Un nome di dominio registrato. È possibile utilizzare Amazon Route 53 come registrar di dominio oppure utilizzare un altro registrar.
- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.
- Associa il dominio personalizzato al servizio App Runner. Per ulteriori informazioni, consulta Gestione di nomi di dominio personalizzati per App Runner.
- Configura il record di convalida del certificato restituito da App Runner sulla tua zona ospitata Route 53 per avviare il processo di convalida del dominio. Per ulteriori informazioni, consulta Convalida DNS in AWS Certificate Manager nella Guida per l'utente di AWS Certificate Manager .

Configurazione di Amazon Route 53 per instradare il traffico a un servizio App Runner

Per configurare Amazon Route 53 per instradare il traffico a un servizio App Runner, completa la seguente procedura.

Instradamento del traffico a un servizio App Runner

1. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome della zona ospitata corrisponde al nome del dominio che desideri utilizzare a cui instradare il traffico.
4. Scegli Crea record.
5. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Immetti il nome di dominio da utilizzare per instradare il traffico verso il servizio App Runner. Il valore predefinito è il nome della hosted zone.

   Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico al tuo servizio App Runner, immetti acme.

   Valore/instradamento traffico a

   Scegli Alias to App Runner Service (Alias per il servizio App Runner), quindi scegli la Regione AWS. Scegli il nome dominio dell'ambiente a cui desideri instradare il traffico.

   Tipo di record

   Accetta il valore predefinito, A — IPv4 address.

   Valutazione dello stato della destinazione

   Accetta il valore di default Sì.
6. Scegli Crea record.

   In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, potrai instradare il traffico al servizio App Runner utilizzando il nome del record di alias creato in questa procedura.

Instradamento del traffico verso un ambiente AWS Elastic Beanstalk

Se lo utilizzi AWS Elastic Beanstalk per distribuire e gestire applicazioni nel AWS cloud, puoi utilizzare Amazon Route 53 per indirizzare il traffico DNS per il tuo dominio, ad esempio example.com, verso un ambiente Elastic Beanstalk nuovo o esistente.

Per instradare il traffico DNS a un ambiente Elastic Beanstalk, consulta le procedure nei seguenti argomenti.

> **Note**
>
> Queste procedure presuppongono l'utilizzo di Route 53 come servizio DNS per il tuo dominio. Se usi un altro servizio DNS, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente per informazioni su come utilizzare Route 53 come provider di servizi DNS per il tuo dominio.

Argomenti

Implementazione di un'applicazione in un ambiente Elastic Beanstalk

Se disponi già di un ambiente Elastic Beanstalk a cui desideri instradare il traffico, passa a Ottenere il nome di dominio per l'ambiente Elastic Beanstalk.

Come creare un'applicazione e implementarla in un ambiente Elastic Beanstalk

- Per informazioni sulla creazione e l'implementazione di un'applicazione in un ambiente Elastic Beanstalk, consulta Nozioni di base sull'uso di Elastic Beanstalk nella Guida per gli sviluppatori di AWS Elastic Beanstalk .

Ottenere il nome di dominio per l'ambiente Elastic Beanstalk

Se conosci già il nome di dominio per il tuo ambiente di Elastic Beanstalk, passa a Creazione di un record Amazon Route 53 che instrada il traffico all'ambiente Elastic Beanstalk.

Come ottenere il nome dominio per l'ambiente Elastic Beanstalk

1. Accedi AWS Management Console e apri la console Elastic Beanstalk all'indirizzo. https://console.aws.amazon.com/elasticbeanstalk/
2. Nell'elenco delle applicazioni, individua l'applicazione a cui desideri instradare il traffico e ottieni il valore dell'URL. Se l'elenco di applicazioni non viene visualizzato, scegli Applications (Applicazioni) nel pannello di navigazione.

   Per ulteriori informazioni sull'URL, consulta Nome di dominio dell'ambiente Elastic Beanstalk nella Guida per gli sviluppatori di Elastic Beanstalk.

Creazione di un record Amazon Route 53 che instrada il traffico all'ambiente Elastic Beanstalk

Un record Amazon Route 53 contiene le impostazioni che controllano il modo in cui il traffico viene instradato al tuo ambiente Elastic Beanstalk. È possibile creare un record CNAME o un record alias, a seconda se il nome di dominio per l'ambiente include la regione, ad esempio us-east-2, in cui è distribuito l'ambiente. I nuovi ambienti includono la regione nel nome di dominio, mentre gli ambienti creati prima dell'inizio del 2016 non la includono. Per un confronto dei record CNAME e alias, vedi Scelta tra record alias e non alias.

Se il nome di dominio non include la regione

Devi creare un record CNAME. Tuttavia, a causa delle limitazioni imposte da DNS, è possibile creare più record CNAME solo per sottodomini, non per il nome di dominio radice. Ad esempio, se il tuo nome di dominio è esempio.com, è possibile creare un record che consente di instradare il traffico per acme.esempio.com al tuo ambiente Elastic Beanstalk, ma non potrai creare un record che consente di instradare il traffico per esempio.com al tuo ambiente Elastic Beanstalk.

Vedi la procedura Come creare un record CNAME per instradare il traffico a un ambiente Elastic Beanstalk.

Se il nome di dominio include la regione

Puoi creare un record alias. Un record alias è specifico di Route 53 e ha due vantaggi significativi rispetto ai record CNAME:

- Puoi creare record alias per il nome di dominio root o per sottodomini. Ad esempio, se il tuo nome di dominio è esempio.com, puoi creare un record che instrada le richieste per esempio.com o per acme.esempio.com al tuo ambiente Elastic Beanstalk.
- Route 53 non prevede costi per le richieste che utilizzano un record alias per instradare il traffico.

Vedi la procedura Come creare un record alias Amazon Route 53 per instradare il traffico a un ambiente Elastic Beanstalk.

Come creare un record CNAME per instradare il traffico a un ambiente Elastic Beanstalk

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome della zona ospitata che desideri utilizzare per instradare il traffico al tuo ambiente Elastic Beanstalk.
4. Scegli Crea record.
5. Scegli Switch per creare rapidamente
6. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Digita il nome di dominio che desideri utilizzare per instradare il traffico al tuo ambiente Elastic Beanstalk. Il valore predefinito è il nome della hosted zone.

   Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico al tuo ambiente, digita acme.

> **Important**
>
> Non puoi creare un record CNAME con lo stesso nome della zona ospitata.

Alias

Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

Valore/instradamento traffico a

Scegli Indirizzo IP o altro valore a seconda del tipo di record e specifica il valore ottenuto durante l'esecuzione della procedura nell'argomento Ottenere il nome di dominio per l'ambiente Elastic Beanstalk. Se hai usato diversi account per creare la tua zona ospitata Route 53 e l'ambiente Elastic Beanstalk, inserisci gli attributi CNAME per l'ambiente Elastic Beanstalk.

Tipo di record

Scegli CNAME.

TTL (secondi)

Accetta il valore di default di 300.

7. Scegli Crea record.

   In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Come creare un record alias Amazon Route 53 per instradare il traffico a un ambiente Elastic Beanstalk

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome della zona ospitata che desideri utilizzare per instradare il traffico al tuo ambiente Elastic Beanstalk.
4. Scegli Crea record.
5. Specifica i seguenti valori:

Policy di routing

Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

Nome record

Digita il nome di dominio che desideri utilizzare per instradare il traffico al tuo ambiente Elastic Beanstalk. Il valore predefinito è il nome della hosted zone.

Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico al tuo ambiente, digita acme.

Valore/instradamento traffico a

Scegli Alias per l'ambiente Elastic Beanstalk, quindi scegli la regione da cui proviene l'endpoint. Scegli il nome dominio dell'ambiente a cui desideri instradare il traffico. Questo è il valore che ottieni quando esegui la procedura nell'argomento Ottenere il nome di dominio per l'ambiente Elastic Beanstalk.

Se hai usato diversi account per creare la tua zona ospitata Route 53 e l'ambiente Elastic Beanstalk, inserisci l'attributo CNAME per l'ambiente Elastic Beanstalk.

Tipo di record

Accetta l' IPv4 indirizzo predefinito, A —.

Valutazione dello stato della destinazione

Accetta il valore di default Sì.

6. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarai in grado di instradare il traffico al tuo ambiente Elastic Beanstalk utilizzando il nome del record alias creato in questa procedura.

Routing del traffico a un load balancer ELB

Se ospiti un sito Web su più EC2 istanze Amazon, puoi distribuire il traffico verso il tuo sito Web tra le istanze utilizzando un sistema di bilanciamento del carico Elastic Load Balancing (ELB). Il servizio ELB ridimensiona automaticamente il load balancer al variare del traffico verso il tuo sito Web nel

corso del tempo. Il load balancer, inoltre, è in grado di monitorare lo stato delle istanze registrate e instradare il traffico di dominio solo alle istanze integre.

Per instradare il traffico di dominio a un load balancer ELB, utilizza Amazon Route 53 per creare un record alias che punti al tuo load balancer. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, ma è possibile creare un record alias sia per il dominio root, ad esempio esempio.com, sia per sottodomini, ad esempio www.esempio.com. (È possibile creare record CNAME solo per sottodomini).

> **Note**
>
> Route 53 non prevede costi per le query di alias rivolte ai bilanciatori del carico ELB o ad altre risorse AWS .

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

- Un load balancer ELB. È possibile usare un ELB Classic, Application o Network Load Balancer. Per ulteriori informazioni, consulta Nozioni di base su Elastic Load Balancer nella Guida per l'utente di Elastic Load Balancer.

  Dai un nome al load balancer che successivamente ti aiuterà a ricordare a cosa serve. Il nome specificato al momento della creazione di un load balancer è il nome che scegli quando crei un record alias nella console Route 53.
- Un nome di dominio registrato. È possibile utilizzare Route 53 come registrar di dominio oppure è possibile utilizzare un altro registrar.
- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Configurazione di Amazon Route 53 per instradare il traffico a un load balancer ELB

Per configurare Amazon Route 53 per instradare il traffico a un load balancer ELB, completa la seguente procedura.

Per instradare il traffico verso un load balancer ELB

1. Se la zona ospitata Route 53 e il load balancer ELB sono stati creati utilizzando lo stesso account, passa alla fase 2.

   Se è stata creata la zona ospitata e il load balancer ELB utilizzando diversi account, eseguire la procedura Come ottenere il nome DNS per un sistema di bilanciamento del carico Elastic Load Balancing per ottenere il nome DNS per il load balancer.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Scegli il nome della zona ospitata che ha il nome di dominio che desideri utilizzare per instradare il traffico verso il load balancer.
5. Scegli Crea record.
6. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

   Nome record

   Digita il nome di dominio o sottodominio che desideri utilizzare per instradare il traffico verso il load balancer ELB. Il valore predefinito è il nome della hosted zone.

   Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico al load balancer, digita acme.

   Alias

   Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

Valore/instradamento traffico a

Scegli Alias per l'applicazione e Classic Load Balancer o Alias per il Network Load Balancer, quindi scegli la regione da cui proviene l'endpoint.

Se hai creato la zona ospitata e il sistema di bilanciamento del carico ELB utilizzando lo stesso AWS account, scegli il nome che hai assegnato al load balancer al momento della creazione.

Se hai creato la zona ospitata e il load balancer ELB utilizzando account diversi, immetti il valore ottenuto nel passaggio 1 di questa procedura.

> **Note**
>
> La console precede il dualstack. al nome DNS dell'applicazione e al Classic Load Balancer solo dallo AWS stesso account. Quando un client, ad esempio un browser Web, richiede l'indirizzo IP per il nome di dominio (example.com) o il nome di sottodominio (www.example.com), il client può richiedere un IPv4 indirizzo (un record A), un indirizzo (un record AAAA) o entrambi IPv4 gli IPv6 indirizzi (in richieste separate con first). IPv6 IPv4 La designazione dualstack. consente a Route 53 di rispondere con l'indirizzo IP appropriato per il load balancer in base al formato dell'indirizzo IP richiesto dal client. Dovrai aggiungere il prefisso dualstack. per Application Load Balancer e Classic Load Balancer dal diverso account.

Tipo di record

Scegli IPv4 A — indirizzo.

Valutazione dello stato della destinazione

Se desideri che tramite Route 53 il traffico venga instradato in base allo stato delle tue risorse, seleziona Sì. Per ulteriori informazioni sul controllo dell'integrità delle tue risorse, consulta Creazione di controlli sanitari su Amazon Route 53 .

7. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarai in grado di instradare il traffico al load balancer utilizzando il nome del record alias che hai creato in questa procedura.

Routing del traffico a un sito Web ospitato in un bucket Amazon S3

Amazon Simple Storage Service (Amazon S3) fornisce un'archiviazione nel cloud sicura, durevole e altamente scalabile. Puoi configurare un bucket S3 in modo che ospiti siti Web statici che possono includere pagine Web e script lato client. (S3 non supporta lo scripting lato server).

Per instradare il traffico di dominio a un bucket S3, utilizza Amazon Route 53 per creare un record alias che punti al tuo bucket. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, ad eccezione del fatto che è possibile creare un record alias sia per il dominio root, ad esempio esempio.com, sia per sottodomini, ad esempio www.esempio.com. È possibile creare record CNAME solo per sottodomini.

> **Note**
>
> Route 53 non addebita alcun costo per le richieste di alias ai bucket S3 o ad altre risorse. AWS

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue. Se non hai mai usato Amazon Route 53 o S3, consulta le informazioni riportate in Nozioni di base su Amazon Route 53, che ti guideranno lungo l'intero processo, tra cui la registrazione di un nome di dominio, nonché la creazione e la configurazione di un bucket S3.

- Un bucket S3 configurato per ospitare un sito Web statico.

  Per ulteriori informazioni, consulta Configurazione di un bucket per l'hosting di un sito Web nella Guida per gli sviluppatori di Amazon Simple Storage Service.

  > **Important**
  >
  > Il bucket deve avere lo stesso nome del dominio o del sottodominio. Ad esempio, se desideri utilizzare il sottodominio acme.esempio.com, il nome del bucket deve essere acme.esempio.com.

  È possibile instradare il traffico per un dominio e i relativi sottodomini, ad esempio esempio.com e www.esempio.com, a un solo bucket. Crea un bucket per il dominio e ogni sottodominio e configura

un solo bucket per reindirizzare il traffico verso i restanti bucket. Per ulteriori informazioni, consulta Nozioni di base su Amazon Route 53.

> **Note**
>
> Si è verificato un bucket S3 configurato come endpoint del sito Web non supporta SSL/TLS, pertanto è necessario instradare il traffico verso la distribuzione CloudFront e utilizzare il bucket S3 come server di origine per la distribuzione.
> Per istruzioni su come creare una CloudFront distribuzione, consulta Creazione di una CloudFront distribuzione e Configurazione di nomi di dominio alternativi e HTTPS nella Guida per l'CloudFront utente in aggiunta a. Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio

- Un nome di dominio registrato. È possibile utilizzare Route 53 come registrar di dominio oppure è possibile utilizzare un altro registrar.
- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Configurazione di Amazon Route 53 per instradare il traffico a un bucket S3

Per configurare Amazon Route 53 per instradare il traffico a un bucket S3 configurato per ospitare un sito Web statico, completa la seguente procedura.

Per instradare il traffico a un bucket S3

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome della zona ospitata che ha il nome di dominio che desideri utilizzare per instradare il traffico verso il bucket S3.
4. Scegli Crea record.
5. Specifica i seguenti valori:

Policy di routing

Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

Nome record

Digita il nome di dominio che desideri utilizzare per instradare il traffico verso il tuo bucket S3. Il valore predefinito è il nome della hosted zone.

Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico al tuo bucket, digita acme.

Alias

Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

Valore/instradamento traffico a

Scegli Alias per l'endpoint del sito Web S3, quindi scegli la regione da cui proviene l'endpoint.

Scegli il bucket con lo stesso nome specificato per Nome record.

L'elenco include un bucket solo se il bucket soddisfa i seguenti requisiti:

- Il nome del bucket è uguale al nome del record che si sta creando.
- Il bucket è configurato come endpoint di sito Web.
- Il bucket è stato creato dall' AWS account corrente.

Se hai creato il bucket utilizzando un AWS account diverso, inserisci il nome della regione in cui hai creato il bucket S3. Per il formato corretto del nome della regione, consulta la colonna Endpoint del sito Web nella tabella Endpoint del sito Web Amazon S3 nella Riferimenti generali di Amazon Web Services.

Tipo di record

Scegli A — indirizzo. IPv4

Valutazione dello stato della destinazione

Accetta il valore di default Sì.

6. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarai in grado di instradare il traffico al tuo bucket S3 utilizzando il nome del record alias creato in questa procedura.

Routing del traffico a un endpoint di interfaccia di Amazon Virtual Private Cloud usando il proprio nome dominio

Puoi utilizzarlo AWS PrivateLink per accedere a servizi selezionati con un endpoint di interfaccia Amazon Virtual Private Cloud (Amazon VPC). Questi servizi includono alcuni AWS servizi, servizi ospitati da altri AWS clienti e partner e servizi Marketplace AWS partner supportati. VPCs

Per instradare il traffico di dominio a un endpoint di interfaccia, utilizza Amazon Route 53 per creare un record alias. Un record alias è un'estensione Route 53 al DNS. È simile a un record CNAME, ma è possibile creare un record alias sia per il dominio root, ad esempio esempio.com, sia per sottodomini, ad esempio www.esempio.com. È possibile creare record CNAME solo per sottodomini.

> **Note**
>
> Route 53 non addebita alcun costo per le richieste di alias agli endpoint di interfaccia o ad altre risorse. AWS

Argomenti

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

- Un endpoint di interfaccia di Amazon VPC. Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.
- Un nome di dominio registrato. È possibile utilizzare Amazon Route 53 come registrar di dominio oppure utilizzare un altro registrar.

- Route 53 come servizio DNS per il dominio. Se record il tuo nome di dominio utilizzando Route 53, configureremo automaticamente Route 53 come servizio DNS per il dominio.

  Per informazioni su come usare Route 53 come provider di servizi DNS per il tuo dominio, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.

Configurazione di Amazon Route 53 per instradare il traffico a un endpoint di interfaccia di Amazon VPC

Per configurare Amazon Route 53 per instradare il traffico a un endpoint di interfaccia di Amazon VPC, completa la seguente procedura.

Per instradare il traffico a un endpoint di interfaccia di Amazon VPC

1. Se la zona ospitata Route 53 e l'endpoint di interfaccia di Amazon VPC sono stati creati utilizzando lo stesso account, passa alla fase 2.

   Se la zona ospitata e l'endpoint di interfaccia sono stati creati utilizzando account diversi, ottenere il nome del servizio per l'endpoint di interfaccia:

   a. Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
   b. Nel pannello di navigazione, seleziona Endpoint.
   c. Nel riquadro a destra, scegliere l'endpoint verso cui si desidera instradare il traffico Internet.
   d. Nel riquadro inferiore, ottenere il valore del nome DNS, ad esempio, vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com.
2. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel pannello di navigazione, scegli Zone ospitate.
4. Scegliere il nome della zona ospitata che ha il nome di dominio da utilizzare per instradare il traffico verso l'endpoint di interfaccia.
5. Scegli Crea record.
6. Specifica i seguenti valori:

   Policy di routing

   Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

Nome record

Digitare il nome di dominio che desideri utilizzare per instradare il traffico verso l'endpoint di interfaccia di Amazon VPC.

Alias

Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

Valore/instradamento traffico a

Scegli Alias per l'endpoint VPC, quindi scegli la regione da cui proviene l'endpoint.

Il modo in cui si specifica il valore per Endpoints dipende dal fatto che la zona ospitata e l'endpoint di interfaccia siano stati creati utilizzando lo stesso AWS account o account diversi:

- Stesso account: scegli l'elenco e individua la categoria Endpoint Amazon VPC. Quindi, scegliere il nome DNS dell'endpoint di interfaccia verso cui instradare il traffico Internet.
- Account diversi: specifica il valore ottenuto nella fase 1 di questa procedura.

Tipo di record

Scegli A — IPv4 indirizzo.

Valutazione dello stato della destinazione

Accetta il valore di default Sì.

7. Scegli Crea record.

In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarà possibile instradare il traffico all'endpoint di interfaccia utilizzando il nome del record alias creato in questa procedura.

Instradamento del traffico verso Amazon WorkMail

Puoi utilizzare Route 53 per indirizzare il traffico verso il tuo dominio WorkMail e-mail Amazon. Il nome della tua zona ospitata su Route 53 (ad esempio example.com) deve corrispondere al nome di un dominio Amazon WorkMail .

> **Note**
>
> Puoi indirizzare il traffico verso un WorkMail dominio Amazon solo per le zone ospitate pubbliche.

Per indirizzare il traffico verso Amazon WorkMail, esegui le seguenti quattro procedure.

Per configurare Amazon Route 53 come servizio DNS e aggiungere un' WorkMail organizzazione Amazon e un dominio e-mail

1. Se non hai registrato il nome di dominio che desideri utilizzare per il tuo indirizzo e-mail (ad esempio nome@esempio.it), registra ora il dominio in modo da sapere che il dominio è disponibile. Per ulteriori informazioni, consulta Registrazione di un nuovo dominio.

   Se Amazon Route 53 non è il servizio DNS per il dominio e-mail che hai aggiunto ad Amazon WorkMail, migra il servizio DNS per il dominio su Route 53. Per ulteriori informazioni, consulta Rendere Amazon Route 53 il servizio DNS per un dominio esistente.
2. Aggiungi un' WorkMail organizzazione Amazon e un dominio e-mail. Per ulteriori informazioni, consulta la sezione Guida introduttiva per nuovi utenti nella Amazon WorkMail Administrator Guide.

Per creare un record TXT Route 53 per Amazon WorkMail

1. Nel pannello di navigazione della WorkMail console Amazon, scegli Domini.
2. Scegli il nome del dominio e-mail, ad esempio example.com, che desideri utilizzare per indirizzare il traffico verso Amazon. WorkMail
3. Aprire un'altra scheda nel browser, quindi aprire la console Route 53.
4. Nella console Route 53, effettua le seguenti operazioni:
   a. Nel pannello di navigazione, scegli Zone ospitate.
   b. Scegli il nome della zona ospitata che desideri utilizzare per il tuo dominio WorkMail e-mail Amazon.
5. Nella WorkMail console Amazon, nella sezione Passaggio 1: verifica la proprietà del dominio, vai alla colonna Hostname e copia la parte del valore che precede il nome del tuo dominio e-mail.

Ad esempio, se il tuo dominio WorkMail e-mail Amazon è example.com e il valore di Hostname è _amazonses.example.com, copia _amazonses.

6. Nella console Route 53, effettua le seguenti operazioni:

   a. Scegli Crea record, quindi scegli Routing semplice.

   b. In Nome incolla il valore copiato nella fase 5.

   c. Per Tipo di record, scegli TXT - Testo.

7. Nella WorkMail console Amazon, per il record TXT, copia il valore della colonna Valore, comprese le virgolette.

8. Nella console Route 53, effettua le seguenti operazioni:

   a. Per Valore/instradamento traffico a, scegli Indirizzo IP o altro valore a seconda del tipo di record e incolla il valore copiato nella fase 7.

      Non cambiare altre impostazioni.

   b. Scegli Create (Crea) .

Per creare un record Route 53 MX per Amazon WorkMail

1. Nella WorkMail console Amazon, nella sezione Passaggio 2: finalizza la configurazione del dominio, vai alla riga con un tipo di record MX e copia il valore della colonna Value.

2. Nella console Route 53, effettua le seguenti operazioni:

   a. Scegli Crea record.

   b. Per Valore/instradamento traffico a, scegli Indirizzo IP o altro valore a seconda del tipo di record e incolla il valore copiato nella fase 1.

   c. Per Tipo di record, scegli MX - Mail Exchange.

      Non cambiare altre impostazioni.

   d. Scegli Crea record.

Per creare quattro record CNAME Route 53 per Amazon WorkMail

1. Nella WorkMail console Amazon, nella sezione Passaggio 2: Finalizza la configurazione del dominio, vai alla prima riga con un tipo di record CNAME. Nella colonna Hostname (Nome host), copiare la parte del valore che precede il nome di dominio e-mail.

   Ad esempio, se il tuo dominio WorkMail e-mail Amazon è example.com e il valore di Hostname è autodiscover.example.com, copia autodiscover.
2. Nella console Route 53, effettua le seguenti operazioni:

   a. Scegli Crea record.

   b. In Nome record incolla il valore copiato nella fase 1.

   c. Per Tipo di record, scegli CNAME - Nome canonico.
3. Nella WorkMail console Amazon, nella prima riga con un tipo di record CNAME, copia il valore della colonna Valore.
4. Nella console Route 53, effettua le seguenti operazioni:

   a. Per Valore/instradamento traffico a, scegli Indirizzo IP o altro valore a seconda del tipo di record e incolla il valore copiato nella fase 3.

      Non cambiare altre impostazioni.

   b. Scegli Crea record.
5. Ripeti i passaggi da 1 a 4 per i record CNAME rimanenti elencati nella WorkMail console Amazon.

Instradamento del traffico verso l'endpoint OpenSearch del dominio Amazon Service

Amazon OpenSearch Service è un servizio gestito che semplifica la distribuzione, il funzionamento e la scalabilità OpenSearch dei cluster in. Cloud AWS Un dominio OpenSearch Service Service è sinonimo di un OpenSearch cluster di servizi. I domini sono cluster con le impostazioni, i tipi di istanza, il numero di istanze e le risorse di archiviazione specificate. Per ulteriori informazioni, consulta Cos'è Amazon OpenSearch Service nella Amazon OpenSearch Service Developer Guide.

Prerequisiti

Per iniziare, è necessario avere a disposizione quanto segue:

Un dominio OpenSearch di servizio con un nome di dominio personalizzato, ad esempio example.com che corrisponde al nome del record Route 53 che desideri creare.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Guida introduttiva all'Amazon OpenSearch Service Developer Guide.
- Creazione di un endpoint personalizzato nell'Amazon OpenSearch Service Developer Guide.

Configurazione di Amazon Route 53 per instradare il traffico verso l'endpoint del dominio Amazon OpenSearch Service

Per utilizzare Route 53 per indirizzare il traffico verso il OpenSearch Servizio, devi prima ottenere l'endpoint di dominio fornito da OpenSearch Service. Questo endpoint dual stack viene fornito solo se l'endpoint personalizzato è abilitato su un dominio di OpenSearch servizio con modalità di rete dual-stack. Per ulteriori informazioni, consulta Creare un endpoint personalizzato nella Amazon OpenSearch Service Developer Guide.

Per indirizzare il traffico verso l'endpoint OpenSearch del servizio

1. Vai a https://aws.amazon.come scegli Accedi alla console.
2. In Analytics, scegli Amazon OpenSearch Service.
3. In Cluster gestiti scegli Domini.
4. Nella pagina Domini scegli il nome del dominio verso cui indirizzare il traffico.
5. Nella pagina dei dettagli del dominio, copia il valore per l'endpoint Domain v2 (dual stack).
6. Apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
7. Nel pannello di navigazione, scegli Zone ospitate.
8. Scegli il nome collegato della zona ospitata per il dominio che desideri utilizzare per indirizzare il traffico verso l'endpoint del OpenSearch servizio. Il nome di dominio deve corrispondere all'endpoint personalizzato definito in OpenSearch Service.
9. Scegli Crea record.

   Per creare i record puoi utilizzare la procedura guidata oppure puoi scegliere Switch to quick create (Passa alla creazione rapida).

10. Specifica i seguenti valori:

    Policy di routing

    Scegliere la policy di routing applicabile. Per ulteriori informazioni, consulta Scegliere una policy di routing.

    Nome record

    Inserisci il nome di dominio che desideri utilizzare per indirizzare il traffico verso l'endpoint del dominio OpenSearch di servizio. Il valore predefinito è il nome della hosted zone.

    Ad esempio, se il nome della zona ospitata è esempio.com e desideri utilizzare acme.esempio.com per instradare il traffico alla tua distribuzione, digita acme.

    Alias

    Se stai usando il metodo di creazione record Creazione rapida, attiva Alias.

    Valore/instradamento traffico a

    Scegli Alias to OpenSearch Service domain endpoint. Scegli la regione in cui è stato creato il dominio di OpenSearch servizio e scegli il valore ottenuto nel passaggio 1.

    Tipo di record

    Scegli un IPv4 indirizzo A o un IPv6 indirizzo AAAA.

    Valutazione dello stato della destinazione

    Accetta il valore di default Sì.

11. Scegli Crea record.

Indirizzamento del traffico verso altre risorse AWS

Di seguito è riportato l'elenco di argomenti in altre guide su come utilizzare Route 53 per instradare il traffico verso tali servizi.

- Utilizzo di AWS Cloud Map nella Guida per l'utente di AWS Cloud Map .
- Gestisci i domini personalizzati nella Guida per gli AWS App Runner sviluppatori.
- Utilizzo di Route 53 come provider DNS nella Guida per l'utente di AWS Transfer Family .
- Utilizzo di Route 53 per puntare un dominio a un'istanza Amazon Lightsail.

Creazione di controlli sanitari su Amazon Route 53

I controlli dell'integrità di Amazon Route 53 monitorano l'integrità e le prestazioni delle applicazioni Web, dei server Web e di altre risorse. Ogni controllo dell'integrità creato è in grado di monitorare uno dei seguenti elementi:

- L'integrità di una risorsa specificata, ad esempio un server Web.
- Lo stato di altri controlli dell'integrità.
- Lo stato di un CloudWatch allarme Amazon.
- Inoltre, con Amazon Application Recovery Controller (ARC), puoi configurare controlli di integrità del controllo del routing con record di failover DNS per gestire il failover del traffico per la tua applicazione. Per ulteriori informazioni, consulta la Amazon Application Recovery Controller (ARC) Developer Guide.

Per una panoramica dei tipi di controlli dell'integrità, consulta Tipi di controlli dell'integrità di Amazon Route 53. Per informazioni su come creare controlli dell'integrità, consulta Creazione e aggiornamento di controlli dell'integrità.

Dopo aver creato un controllo dell'integrità, è possibile ottenere lo stato del controllo, ottenere notifiche quando lo stato cambia e configurare il failover DNS:

Ottenere lo stato del controllo dell'integrità e le notifiche

Puoi visualizzare lo stato corrente e recente dei controlli controllo dell'integrità sulla console Route 53. Puoi anche gestire i controlli sanitari in modo programmatico tramite una delle AWS SDKs, le o l' AWS Command Line Interface AWS Tools for Windows PowerShell API Route 53.

Se desideri ricevere una notifica quando lo stato di un controllo sanitario cambia, puoi configurare un CloudWatch allarme Amazon per ogni controllo sanitario.

Per ulteriori informazioni sulla visualizzazione dello stato del controllo dell'integrità e la ricezione di notifiche, consulta Monitoraggio dello stato del controllo dell'integrità e ricezione di notifiche.

Configurazione di un failover DNS

Se si dispone di più risorse che eseguono la stessa funzione, è possibile configurare il failover DNS in modo che Route 53 instraderà il traffico da una risorsa non integra a una risorsa integra. Ad esempio, se disponi di due server Web e un server Web diventa non integro, Route 53 può

instradare il traffico verso l'altro server Web. Per ulteriori informazioni, consulta Configurazione di un failover DNS.

Argomenti

Tipi di controlli dell'integrità di Amazon Route 53

È possibile creare i seguenti tipi di controlli dell'integrità per Amazon Route 53:

I controlli dell'integrità in grado di monitorare un endpoint

È possibile configurare un controllo dell'integrità che monitora un endpoint specificato dall'indirizzo IP o dal nome di dominio. A intervalli regolari specificati, Route 53 inoltra le richieste automatizzate tramite Internet alla tua applicazione, server o altre risorse per verificare che sia raggiungibile, disponibile e funzionante. Facoltativamente, è possibile configurare il controllo dell'integrità per effettuare richieste simili a quelle dei tuoi utenti, come richiedere una pagina Web da un URL specifico.

Controlli dello stato che monitorano altri controlli dell'integrità (controlli dell'integrità calcolati)

È possibile creare un controllo dell'integrità che monitora se Route 53 considera altri controlli dell'integrità integri o non integri. Una situazione in cui questo può risultare utile è quando si dispone di più risorse che eseguono la stessa funzione, ad esempio più server Web, e la preoccupazione principale è se un numero minimo di risorse sono integre. È possibile creare un controllo dell'integrità per ciascuna risorsa senza configurare notifiche per i controlli dell'integrità. Quindi è possibile creare un controllo dell'integrità che monitora lo stato degli altri controlli dell'integrità e che fornisce una notifica solo quando il numero di risorse Web disponibili scende al di sotto di una determinata soglia.

Controlli sanitari che monitorano gli CloudWatch allarmi

Puoi creare CloudWatch allarmi che monitorano lo stato delle CloudWatch metriche, come il numero di eventi di lettura limitati per un database Amazon DynamoDB o il numero di host Elastic Load Balancing considerati integri. Dopo aver creato un allarme, puoi creare un controllo dello stato che monitora lo stesso flusso di dati che monitora l'allarme. CloudWatch

Per migliorare la resilienza e la disponibilità, Route 53 non aspetta che l' CloudWatchallarme entri in funzione. `ALARM` Lo stato di un controllo sanitario cambia da integro a non integro in base al flusso di dati e ai criteri indicati nell' CloudWatch allarme.

Route 53 supporta gli CloudWatch allarmi con le seguenti funzionalità:

- Parametri con risoluzione standard. I parametri ad alta risoluzione non sono supportati. Per ulteriori informazioni, consulta i parametri ad alta risoluzione nella Amazon CloudWatch User Guide.
- Statistiche: media, minima, massima, somma e. SampleCount Le statistiche estese non sono supportate.
- Route 53 non supporta gli allarmi "M di N" . Per ulteriori informazioni, consulta la sezione Valutazione di un allarme nella CloudWatch guida di Amazon.
- Un controllo sanitario può monitorare solo un CloudWatch allarme presente nello stesso AWS account del controllo sanitario.
- Route 53 non supporta gli allarmi che utilizzano la matematica metrica per interrogare più metriche. CloudWatch

Controller di routing Amazon Application Recovery Controller (ARC)

I controlli Health in ARC sono associati ai controlli di routing, che sono semplici interruttori di accensione/spegnimento. È possibile configurare ogni controllo dell'integrità del controllo di routing con un record DNS di failover. Quindi puoi semplicemente aggiornare i controlli di routing in ARC per reindirizzare il traffico e eseguire il failover delle applicazioni, ad esempio tra zone o aree di disponibilità. AWS Per ulteriori informazioni, consulta il controllo del routing in ARC nella guida per sviluppatori ARC.

Come Amazon Route 53 determina se un controllo dell'integrità è integro

Il metodo che Amazon Route 53 impiega per determinare se un controllo dell'integrità è integro dipende dal tipo di controllo dell'integrità.

Argomenti

Come Route 53 determina lo stato dei controlli dell'integrità che monitorano un endpoint

Route 53 dispone di strumenti di controllo dell'integrità localizzati in sedi in tutto il mondo. Quando si crea un controllo dell'integrità che monitora un endpoint, gli strumenti di controllo dell'integrità iniziano a inviare le richieste verso l'endpoint specificato dall'utente per determinare se l'endpoint è integro. È possibile scegliere quali sedi si desidera che Route 53 utilizzi ed è possibile specificare l'intervallo tra controlli: ogni 10 secondi o ogni 30 secondi. Gli strumenti di controllo dell'integrità di Route 53 in diversi data center non sono coordinati tra loro, perciò potrai talvolta vedere diverse richieste al secondo indipendentemente dall'intervallo di tempo scelto, seguito da alcuni secondi, senza controlli dell'integrità.

Ogni strumento di controllo dell'integrità valuta l'integrità dell'endpoint in base a due valori:

- Tempo di risposta. Una risorsa può essere lenta nel rispondere o non essere in grado di rispondere a una richiesta di controllo dell'integrità per una serie di motivi. Ad esempio, la risorsa viene interrotta per manutenzione, è sottoposta a un attacco Distributed Denial of Service (DDoS) o la rete è inattiva.
- Se l'endpoint risponde a una serie di controlli dell'integrità consecutivi specificati (la soglia di errore)

Route 53 aggrega i dati provenienti dagli strumenti di controllo dell'integrità e determina se l'endpoint è integro:

- Se più del 18% degli strumenti di controllo dell'integrità segnala che un endpoint è integro, Route 53 lo considererà integro.
- Se meno del 18% degli strumenti di controllo dell'integrità segnala che un endpoint è integro, Route 53 lo considererà non integro.

Il valore di 18% è stato scelto per garantire che gli strumenti di controllo dell'integrità in più regioni considerino l'endpoint integro. In questo modo si impedisce che un endpoint venga considerato non integro solo perché le condizioni di rete hanno isolato l'endpoint da alcune location di verifica dello stato. Questo valore potrebbe cambiare in una versione futura.

Il tempo di risposta che un singolo strumento di controllo dell'integrità impiega per determinare se un endpoint è integro dipende dal tipo di controllo dell'integrità:

- Controlli dell'integrità HTTP e HTTPS: Route 53 deve essere in grado di stabilire una connessione TCP con l'endpoint entro quattro secondi. Inoltre, l'endpoint deve rispondere con un codice di stato HTTP 2xx o 3xx entro due secondi dopo aver eseguito la connessione.

  > **Note**
  >
  > I controlli dell'integrità HTTPS non convalidano i certificati SSL/TLS, pertanto i controlli non hanno esito negativo se un certificato non è valido o è scaduto.

- Controlli dell'integrità TCP: Route 53 deve essere in grado di stabilire una connessione TCP con l'endpoint entro dieci secondi.
- Controlli dell'integrità HTTP e HTTPS con stringa corrispondente: come per i controlli dell'integrità HTTP e HTTPS, Route 53 deve poter stabilire una connessione TCP con l'endpoint entro quattro secondi e l'endpoint deve rispondere con un codice di stato HTTP 2xx o 3xx entro due secondi dopo aver eseguito la connessione.

  Dopo che uno strumento di controllo dell'integrità di Route 53 riceve il codice di stato HTTP, deve ricevere il corpo della risposta dall'endpoint entro due secondi. Route 53 cerca una stringa specificata dall'utente nel corpo della risposta. La stringa deve essere visualizzata interamente nei primi 5.120 byte del corpo della risposta o l'endpoint non supera il controllo dell'integrità. Se stai utilizzando la console Route 53, devi specificare la stringa nel campo Stringa di ricerca . Se stai utilizzando l'API Route 53, devi specificare la stringa nell'elemento `SearchString` quando crei il controllo dell'integrità.

Per i controlli di integrità che monitorano un endpoint (eccetto i controlli di integrità TCP), se la risposta dall'endpoint include delle intestazioni, le intestazioni devono essere nel formato definito in RFC723 0, Hypertext Transfer Protocol (HTTP/1.1): Sintassi e routing dei messaggi, sezione 3.2, «Campi di intestazione».

Route 53 considera un nuovo controllo dell'integrità integro finché non c'è un numero sufficiente di dati per determinare lo stato effettivo, integro o non integro. Se hai scelto la possibilità di invertire lo stato del controllo dell'integrità, Route 53 considera un nuovo controllo dell'integrità non integro finché non c'è un numero sufficiente di dati.

Come Route 53 determina lo stato dei controlli dell'integrità che monitorano altri controlli dell'integrità

Un controllo dell'integrità è in grado di monitorare lo stato di altri controlli dell'integrità; questo tipo di controllo è noto come controllo dell'integrità calcolato. Il controllo dell'integrità che si occupa del monitoraggio è il controllo dell'integrità padre e i controlli dell'integrità che vengono monitorati sono i controlli dell'integrità figlio. Un controllo dell'integrità padre può monitorare lo stato di un massimo di 255 controlli dell'integrità figlio. Ecco come funziona il monitoraggio:

- Route 53 aggiunge il numero di controlli dell'integrità figli che sono considerati integri.
- Route 53 confronta quindi questo numero con il numero di controlli dell'integrità figli che devono essere integri affinché lo stato del controllo dell'integrità padre sia considerato integro.

Per ulteriori informazioni, consulta Monitoraggio di altri controlli dell'integrità (controlli dell'integrità calcolati) in Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.

Route 53 considera un nuovo controllo dell'integrità integro finché non c'è un numero sufficiente di dati per determinare lo stato effettivo, integro o non integro. Se hai scelto la possibilità di invertire lo stato del controllo dell'integrità, Route 53 considera un nuovo controllo dell'integrità non integro finché non c'è un numero sufficiente di dati. Se si inverte il controllo dello stato, Route 53 considera un endpoint sano come malsano e viceversa.

In che modo Route 53 determina lo stato dei controlli di integrità che monitorano gli allarmi CloudWatch

Quando si crea un controllo di integrità basato su un CloudWatch allarme, Route 53 monitora il flusso di dati per l'allarme corrispondente anziché monitorare lo stato dell'allarme. Se il flusso di dati indica che lo stato dell'allarme è OK, il controllo dell'integrità è considerato integro. Se il flusso

di dati indica che lo stato è Alarm (Allarme), il controllo dell'integrità è considerato non integro. Se il flusso di dati non offre informazioni sufficienti per determinare lo stato dell'allarme, lo stato del controllo dell'integrità dipende dalle impostazioni per Health check status (Stato del controllo dell'integrità): integro, non integro o ultimo stato noto. (Nell'API Route 53, questa impostazione è `InsufficientDataHealthStatus`).

Route 53 non supporta gli allarmi tra account CloudWatch .

> **Note**
>
> Poiché i controlli di integrità di Route 53 monitorano CloudWatch i flussi di dati anziché lo stato degli CloudWatch allarmi, non puoi forzare la modifica dello stato di un controllo di integrità utilizzando l'operazione API. CloudWatch SetAlarmState

Route 53 considera un nuovo controllo dell'integrità integro finché non c'è un numero sufficiente di dati per determinare lo stato effettivo, integro o non integro. Se hai scelto la possibilità di invertire lo stato del controllo dell'integrità, Route 53 considera un nuovo controllo dell'integrità non integro finché non c'è un numero sufficiente di dati. Se si inverte il controllo dello stato, Route 53 considera un endpoint sano come non sano e viceversa.

Creazione, aggiornamento ed eliminazione dei controlli dell'integrità

> **Important**
>
> Se stai aggiornando o eliminando controlli dell'integrità associati a record, esamina le operazioni in Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS prima di continuare.

Questa sezione tratta i seguenti argomenti relativi alla gestione dei controlli di integrità della Route 53:

1. Creazione e aggiornamento dei controlli sanitari:
   - Scopri come creare e aggiornare i controlli sanitari utilizzando la console Route 53.
   - Comprendi i valori che devi specificare quando crei o aggiorni i controlli di integrità, come il monitoraggio degli endpoint, il protocollo, l'indirizzo IP, il nome di dominio e le opzioni di configurazione avanzate.

2. Valori visualizzati durante la creazione di un controllo sanitario:
   - Scopri i valori visualizzati dalla console Route 53 in base ai dati immessi durante la creazione di un controllo dello stato, ad esempio l'URL completo o l'indirizzo IP e la porta.
3. Aggiornamento dei controlli sanitari per le modifiche agli CloudWatch allarmi:
   - Scopri come aggiornare un controllo sanitario quando modifichi le impostazioni dell' CloudWatch allarme associato.
4. Eliminazione dei controlli sanitari:
   - Segui la procedura per eliminare i controlli sanitari utilizzando la console Route 53.
5. Aggiornamento o eliminazione dei controlli di integrità quando è configurato il failover DNS:
   - Scopri le attività consigliate da eseguire durante l'aggiornamento o l'eliminazione dei controlli di integrità associati ai record DNS per garantire una corretta configurazione di routing e failover.
6. Configurazione delle regole del router e del firewall:
   - Scopri come configurare le regole del router e del firewall per consentire il traffico in entrata proveniente dai controllori sanitari della Route 53, garantendo il corretto funzionamento dei controlli.

Seguendo le informazioni fornite in questa sezione, puoi creare, aggiornare ed eliminare in modo efficace i controlli di integrità di Route 53, gestirne la configurazione e garantire la corretta integrazione con le politiche di failover e routing DNS.

Argomenti

Creazione e aggiornamento di controlli dell'integrità

La procedura seguente descrive come creare e aggiornare i controlli dell'integrità utilizzando la console Route 53.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per creare o aggiornare un controllo sanitario

1. In caso di aggiornamento o eliminazione di controlli dell'integrità già associati a record, eseguire le attività consigliate in Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS.
2. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
4. Se desideri aggiornare un controllo sanitario esistente, scegli l'ID collegato del controllo sanitario, quindi scegli Modifica.

   Se desideri creare un controllo sanitario, scegli Crea controllo sanitario.
5. Immetti i valori applicabili. Alcuni valori non possono essere modificati dopo aver creato un controllo dell'integrità. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.
6. Scegli Crea controllo dello stato.

> **Note**
>
> Route 53 considera un nuovo controllo dell'integrità integro finché non c'è un numero sufficiente di dati per determinare lo stato effettivo, integro o non integro.

7. Associa il controllo dell'integrità a uno o più record di Route 53. Per ulteriori informazioni sulla creazione e l'aggiornamento di record, consulta Utilizzo dei record.

Old console

Per creare o aggiornare un controllo sanitario

1. In caso di aggiornamento o eliminazione di controlli dell'integrità già associati a record, eseguire le attività consigliate in Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS.
2. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
4. Se si desidera aggiornare un controllo dell'integrità, selezionarlo e scegliere Edit Health Check (Modifica controllo dell'integrità).

   Se si desidera creare un controllo dell'integrità, scegliere Create Health Check (Crea controllo dell'integrità). Per ulteriori informazioni su ciascuna impostazione, sposta il puntatore del mouse sulla rispettiva etichetta per visualizzare una descrizione.
5. Immetti i valori applicabili. Alcuni valori non possono essere modificati dopo aver creato un controllo dell'integrità. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.
6. Scegli Create Health Check (Crea controllo dell'integrità).

> **Note**
>
> Route 53 considera un nuovo controllo dell'integrità integro finché non c'è un numero sufficiente di dati per determinare lo stato effettivo, integro o non integro. Se hai scelto la possibilità di invertire lo stato del controllo dell'integrità, Route 53 considera

un nuovo controllo dell'integrità non integro finché non c'è un numero sufficiente di dati.

7. Associa il controllo dell'integrità a uno o più record di Route 53. Per ulteriori informazioni sulla creazione e l'aggiornamento di record, consulta Utilizzo dei record.

Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità

Quando crei o aggiorni controlli dell'integrità, devi specificare i valori applicabili. Alcuni valori non possono essere modificati dopo aver creato un controllo dell'integrità.

Argomenti

- Monitoraggio di un endpoint
- Monitoraggio di altri controlli dell'integrità (controlli dell'integrità calcolati)
- Monitoraggio di un allarme CloudWatch
- Configurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint))
- Ricevere una notifica quando il controllo dell'integrità ha esito negativo

Nome

Facoltativo ma consigliato: il nome che si desidera assegnare al controllo dell'integrità. Se specifichi un valore per Nome, Route 53 aggiunge un tag al controllo dell'integrità, assegna il valore Nome alla chiave di tag e assegna il valore specificato al valore del tag. Il valore del tag Nome viene visualizzato nell'elenco dei controlli dell'integrità nella console Route 53, che consente di distinguere tra loro i controlli dell'integrità.

Per ulteriori informazioni su tagging e controlli dell'integrità, consulta Denominazione e tagging di controlli dell'integrità.

Cosa monitorare

Se si desidera che questo controllo dell'integrità monitori lo stato di un endpoint o altri controlli dell'integrità:

- Endpoint: Route 53 monitora lo stato di un endpoint da te specificato. È possibile specificare l'endpoint tramite il nome di dominio o un indirizzo IP e una porta.

> **Note**
>
> Se si specifica un dispositivo diverso dall'AWS endpoint, viene applicato un costo aggiuntivo. Per ulteriori informazioni, inclusa una definizione di endpoint AWS , consulta "Controlli dell'integrità" nella pagina Prezzi di Route 53.

- Stato di altri controlli dell'integrità (controllo dell'integrità calcolato): Route 53 determina se il controllo dell'integrità è integro in base allo stato di altri controlli dell'integrità da te specificati. È possibile anche specificare quanti controlli dell'integrità devono essere integri affinché questo controllo dell'integrità sia considerato integro.
- Flusso di dati sullo stato dell' CloudWatch allarme: Route 53 determina se questo controllo di integrità è corretto monitorando il flusso di dati per rilevare eventuali CloudWatch allarmi.

Monitoraggio di un endpoint

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Se desideri che questo controllo dell'integrità monitori un endpoint, specifica i valori seguenti:

- Specificare gli endpoint per
- Indirizzo IP
- Nome dominio

Specifica endpoint per

Se desideri specificare l'endpoint utilizzando un indirizzo IP o utilizzando un nome di dominio.

Dopo aver creato un controllo dell'integrità, non puoi modificare il valore di Specify endpoint by (Specifica endpoint per).

Indirizzo IP (solo "Specify endpoint by IP address" (Specifica endpoint in base all'indirizzo IP) Only)

Scegli il protocollo nel menu a discesa, inserisci l'indirizzo IP, la porta e il percorso nella casella di testo.

- Il protocollo può essere uno dei seguenti:

  HTTP: Route 53 prova a stabilire una connessione TCP. Se ciò avviene, Route 53 invia una richiesta HTTP e resta in attesa di un codice di stato HTTP 2xx o 3xx.
- HTTPS: Route 53 prova a stabilire una connessione TCP. Se ciò avviene, Route 53 invia una richiesta HTTPS e resta in attesa di un codice di stato HTTP 2xx o 3xx.

  > **Important**
  >
  > Se scegli HTTPS, l'endpoint deve supportare TLS v1.0, v1.1 o v1.2.

  Se scegli HTTPS per il valore di Protocol (Protocollo), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.
- TCP: Route 53 prova a stabilire una connessione TCP.

Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di Protocol (Protocollo).

Per l'indirizzo IP puoi inserire un IPv6 indirizzo IPv4 or dell'endpoint su cui desideri che Route 53 esegua i controlli di integrità, se hai scelto Specificare l'endpoint per indirizzo IP.

Route 53 non è in grado di verificare l'integrità di endpoint per cui l'indirizzo IP è in intervalli locali, privati, non instradabili o multicast. Per ulteriori informazioni sugli indirizzi IP per cui non è possibile creare controlli dell'integrità, consulta i seguenti documenti:

- RFC 5735, indirizzi per uso speciale IPv4
- RFC 6598, prefisso riservato IANA per lo spazio di indirizzi condiviso IPv4 .
- RFC 5156, indirizzi per uso speciale IPv6

Se l'endpoint è un' EC2 istanza Amazon, ti consigliamo di creare un indirizzo IP elastico, associarlo all' EC2 istanza e specificare l'indirizzo IP elastico. In questo modo l'indirizzo IP di un'istanza non cambia mai. Per ulteriori informazioni, consulta Elastic IP address (EIP) nella Amazon EC2 User Guide.

Se elimini l' EC2 istanza Amazon, assicurati di eliminare anche il controllo dello stato associato all'EIP. Per ulteriori informazioni, consulta Best practice per i controlli dell'integrità di Amazon Route 53.

> **Note**
>
> Se specifichi un dispositivo diverso dall'AWS endpoint, verrà applicato un costo aggiuntivo. Per ulteriori informazioni, inclusa una definizione di endpoint AWS , consulta "Controlli dell'integrità" nella pagina Prezzi di Route 53.

Per la porta inserite la porta sull'endpoint su cui desiderate che Route 53 esegua i controlli di integrità.

Per il percorso (solo protocolli HTTP e HTTPS) inserisci il percorso che desideri che Route 53 richieda durante i controlli di integrità. Il percorso può essere qualsiasi valore per il quale l'endpoint restituirà un codice di stato H TTP di 2xx o 3xx quando l'endpoint è integro, ad esempio .html? file /docs/route53-health-check.html. You can also include query string parameters, for example, /welcome language=jp&login=y. Se non includi una barra iniziale (/), Route 53 ne aggiunge automaticamente una.

Nome di dominio (solo "Specify endpoint by domain name" (Specifica endpoint utilizzando il nome di dominio), tutti i protocolli)

Il nome di dominio (esempio.com) o il nome di sottodominio (backend.esempio.com) degli endpoint su cui desideri che Route 53 esegua dei controlli dell'integrità, se scegli Specifica endpoint utilizzando il nome dominio.

Se scegli di specificare l'endpoint del nome di dominio, Route 53 invia una query DNS per risolvere il nome di dominio specificato in Nome dominio all'intervallo specificato in Intervallo

richiesta. Utilizzando un indirizzo IP che il DNS restituisce, Route 53 controlla l'integrità dell'endpoint.

> **Note**
>
> Se si specifica l'endpoint per nome di dominio, Route 53 lo utilizza solo IPv4 per inviare controlli sanitari all'endpoint. Se non esiste un record con un tipo di A per il nome specificato per il Domain name (Nome di dominio), il controllo ha esito negativo con un errore di tipo "risoluzione DNS non riuscita".

Se si desidera controllare lo stato di record di failover, geolocalizzazione, geoprossimità, latenza, multivalore o ponderati e si sceglie di specificare l'endpoint per nome di dominio, è consigliabile creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Per il valore di Domain Name (Nome dominio), specifica il nome di dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (www.esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Inoltre, se il valore di Protocollo è HTTP o HTTPS, Route 53 invia il valore di Nome dominio nell'intestazione `Host` come descritto in Nome host, precedentemente in questo elenco. Se il valore di Protocollo è TCP, Route 53 non passa un'intestazione `Host`.

> **Note**
>
> Se si specifica un dispositivo diverso dall'AWS endpoint, viene applicato un costo aggiuntivo. Per ulteriori informazioni, inclusa una definizione di endpoint AWS , consulta "Controlli dell'integrità" nella pagina Prezzi di Route 53.

Old console

Se desideri che questo controllo dell'integrità monitori un endpoint, specifica i valori seguenti:

- Specifica endpoint per
- Protocollo
- Indirizzo IP
- Host name (Nome host)
- Porta
- Nome dominio
- Path

Specifica endpoint per

Se desideri specificare l'endpoint utilizzando un indirizzo IP o utilizzando un nome di dominio.

Dopo aver creato un controllo dell'integrità, non puoi modificare il valore di Specify endpoint by (Specifica endpoint per).

Protocollo

Il metodo che desideri che Route 53 utilizzi per controllare l'integrità del tuo endpoint:

- HTTP: Route 53 prova a stabilire una connessione TCP. Se ciò avviene, Route 53 invia una richiesta HTTP e resta in attesa di un codice di stato HTTP 2xx o 3xx.
- HTTPS: Route 53 prova a stabilire una connessione TCP. Se ciò avviene, Route 53 invia una richiesta HTTPS e resta in attesa di un codice di stato HTTP 2xx o 3xx.

> **Important**
>
> Se scegli HTTPS, l'endpoint deve supportare TLS v1.0, v1.1 o v1.2.

Se scegli HTTPS per il valore di Protocol (Protocollo), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

- TCP: Route 53 prova a stabilire una connessione TCP.

Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di Protocol (Protocollo).

Indirizzo IP (solo "Specify endpoint by IP address" (Specifica endpoint in base all'indirizzo IP) Only)

L' IPv6 indirizzo IPv4 o dell'endpoint su cui desideri che Route 53 esegua i controlli di integrità, se hai scelto Specificare l'endpoint per indirizzo IP.

Route 53 non è in grado di verificare l'integrità di endpoint per cui l'indirizzo IP è in intervalli locali, privati, non instradabili o multicast. Per ulteriori informazioni sugli indirizzi IP per cui non è possibile creare controlli dell'integrità, consulta i seguenti documenti:

- RFC 5735, indirizzi per uso speciale IPv4
- RFC 6598, prefisso riservato IANA per lo spazio di indirizzi condiviso IPv4 .
- RFC 5156, indirizzi per uso speciale IPv6

Se l'endpoint è un' EC2 istanza Amazon, ti consigliamo di creare un indirizzo IP elastico, associarlo all' EC2 istanza e specificare l'indirizzo IP elastico. In questo modo l'indirizzo IP di un'istanza non cambia mai. Per ulteriori informazioni, consulta Elastic IP address (EIP) nella Amazon EC2 User Guide.

Se elimini l' EC2 istanza Amazon, assicurati di eliminare anche il controllo dello stato associato all'EIP. Per ulteriori informazioni, consulta Best practice per i controlli dell'integrità di Amazon Route 53.

> **Note**
>
> Se specifichi un dispositivo diverso dall'AWS endpoint, verrà applicato un costo aggiuntivo. Per ulteriori informazioni, inclusa una definizione di endpoint AWS , consulta "Controlli dell'integrità" nella pagina Prezzi di Route 53.

Nome host (solo "Specify endpoint by IP address" (Specifica endpoint in base all'indirizzo IP), solo protocolli HTTP e HTTPS)

Il valore che desideri che Route 53 passi nell'intestazione `Host` nei controlli dell'integrità HTTP e HTTPS. Questo è in genere il nome DNS completo del sito Web su cui desideri che Route 53 esegua controlli dell'integrità. Quando Route 53 controlla lo stato di un endpoint, ecco come costruisce l'intestazione `Host`:

- Se specifichi un valore **80** per Porta e HTTP per Protocollo, Route 53 invia all'endpoint una intestazione `Host` che contiene il valore di Nome host.
- Se specifichi un valore **443** per Porta e HTTPS per Protocollo, Route 53 invia all'endpoint una intestazione `Host` che contiene il valore di Nome host.
- Se si specifica un altro valore per Port e HTTP o HTTPS per Protocol, Route 53 passa all'endpoint un'**`Host`**intestazione che contiene il valore:. ***`Host name`*** *`Port`*

Se scegli di specificare l'endpoint in base all'indirizzo IP e non specifichi un valore per Nome host, Route 53 sostituisce il valore di Indirizzo IP nell'intestazione `Host` in ciascuno dei casi precedenti.

Porta

La porta dell'endpoint su cui desideri che Route 53 esegua i controlli dell'integrità.

Nome di dominio (solo "Specify endpoint by domain name" (Specifica endpoint utilizzando il nome di dominio), tutti i protocolli)

Il nome di dominio (esempio.com) o il nome di sottodominio (backend.esempio.com) degli endpoint su cui desideri che Route 53 esegua dei controlli dell'integrità, se scegli Specifica endpoint utilizzando il nome dominio.

Se scegli di specificare l'endpoint del nome di dominio, Route 53 invia una query DNS per risolvere il nome di dominio specificato in Nome dominio all'intervallo specificato in Intervallo richiesta. Utilizzando un indirizzo IP che il DNS restituisce, Route 53 controlla l'integrità dell'endpoint.

> **Note**
>
> Se si specifica l'endpoint per nome di dominio, Route 53 lo utilizza solo IPv4 per inviare controlli sanitari all'endpoint. Se non esiste un record con un tipo di A per il nome specificato per il Domain name (Nome di dominio), il controllo ha esito negativo con un errore di tipo "risoluzione DNS non riuscita".

Se si desidera controllare lo stato di record di failover, geolocalizzazione, geoprossimità, latenza, multivalore o ponderati e si sceglie di specificare l'endpoint per nome di dominio, è consigliabile creare un controllo dell'integrità separato per ciascun endpoint. Ad esempio, puoi creare un controllo dell'integrità per ciascun server HTTP che gestisce contenuti per www.esempio.com. Per il valore di Domain Name (Nome dominio), specifica il nome di

dominio del server (ad esempio, us-east-2-www.esempio.com), anziché il nome dei record (www.esempio.com).

> **Important**
>
> In questa configurazione, se crei un controllo dell'integrità per il quale il valore di Domain Name (Nome dominio) corrisponde al nome dei record e quindi associ il controllo dell'integrità a quei record, i risultati del controllo dell'integrità saranno imprevedibili.

Inoltre, se il valore di Protocollo è HTTP o HTTPS, Route 53 invia il valore di Nome dominio nell'intestazione `Host` come descritto in Nome host, precedentemente in questo elenco. Se il valore di Protocollo è TCP, Route 53 non passa un'intestazione `Host`.

> **Note**
>
> Se si specifica un dispositivo diverso dall'AWS endpoint, viene applicato un costo aggiuntivo. Per ulteriori informazioni, inclusa una definizione di endpoint AWS , consulta "Controlli dell'integrità" nella pagina Prezzi di Route 53.

Percorso (solo protocolli HTTP e HTTPS)

Il percorso che desideri che Route 53 richiede quando si eseguono controlli dell'integrità. Il percorso può essere qualsiasi valore per il quale l'endpoint restituirà un codice di stato HTTP di `2xx` o `3xx` quando è integro, ad esempio il file `/docs/route53-health-check.html`. È inoltre possibile includere i parametri di stringa di query, ad esempio, `/welcome.html?language=jp&login=y`. Se non includi una barra (`/`), Route 53 ne aggiunge automaticamente una.

Monitoraggio di altri controlli dell'integrità (controlli dell'integrità calcolati)

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Se si desidera che il controllo dell'integrità monitori lo stato di altri controlli dell'integrità, specifica i seguenti valori:

- Controlli dello stato da monitorare
- Segnala integro quando

Controlli dello stato da monitorare

I controlli dell'integrità che desideri che Route 53 monitori per determinare lo stato di questo controllo dell'integrità.

Puoi aggiungere fino a 256 controlli dell'integrità per Health checks to monitor (Controlli dello stato da monitorare). Per rimuovere un controllo dell'integrità dall'elenco, seleziona la x a destra dell'evidenziazione per quel controllo dell'integrità.

> **Note**
>
> Non è possibile configurare un controllo dell'integrità calcolato per monitorare lo stato di altri controlli dell'integrità calcolati.

Se disabiliti un controllo dell'integrità monitorato da un controllo dell'integrità calcolato, Route 53 considera integro il controllo dell'integrità disabilitato dato che calcola se il controllo dell'integrità calcolato è integro. Se desideri che il controllo dell'integrità disabilitato sia considerato non integro, scegli la casella di controllo Invert health check status (Inverti lo stato di controllo dell'integrità).

Segnala integro quando

Il calcolo che desideri che Route 53 esegua per determinare se questo controllo dell'integrità è integro:

- Segnala integro quando almeno x degli y controlli dell'integrità sono integri: Route 53 considera questo controllo dell'integrità integro quando il numero specificato di controlli dell'integrità aggiunti a Controlli dell'integrità da monitorare sono integri. Tieni presente quanto segue:
  - Se specifichi un numero maggiore del numero di controlli dell'integrità riportato in Controlli dell'integrità da monitorare, Route 53 considera sempre questo controllo dell'integrità non integro.
  - Se specifichi 0, Route 53 considera sempre questo controllo dell'integrità integro.
- Segnala integro quando tutti i controlli dell'integrità sono integri (AND): Route 53 considera questo controllo dell'integrità integro solo quando tutti i controlli dell'integrità aggiunti a Controlli dell'integrità da monitorare sono integri.
- Segnala integro quando uno o più controlli dell'integrità sono integri (OR): Route 53 considera questo controllo dell'integrità integro quando almeno uno dei controlli dell'integrità aggiunto a Controlli dell'integrità da monitorare è integro.

Old console

Se si desidera che il controllo dell'integrità monitori lo stato di altri controlli dell'integrità, specifica i seguenti valori:

- Controlli dello stato da monitorare
- Segnala integro quando
- Inverti stato del controllo dell'integrità
- Disabilitato

Controlli dello stato da monitorare

I controlli dell'integrità che desideri che Route 53 monitori per determinare lo stato di questo controllo dell'integrità.

Puoi aggiungere fino a 256 controlli dell'integrità per Health checks to monitor (Controlli dello stato da monitorare). Per rimuovere un controllo dell'integrità dall'elenco, seleziona la x a destra dell'evidenziazione per quel controllo dell'integrità.

> **Note**
>
> Non è possibile configurare un controllo dell'integrità calcolato per monitorare lo stato di altri controlli dell'integrità calcolati.

Se disabiliti un controllo dell'integrità monitorato da un controllo dell'integrità calcolato, Route 53 considera integro il controllo dell'integrità disabilitato dato che calcola se il controllo dell'integrità calcolato è integro. Se desideri che il controllo dell'integrità disabilitato sia considerato non integro, scegli la casella di controllo Invert health check status (Inverti lo stato di controllo dell'integrità).

Segnala integro quando

Il calcolo che desideri che Route 53 esegua per determinare se questo controllo dell'integrità è integro:

- Segnala integro quando almeno x degli y controlli dell'integrità sono integri: Route 53 considera questo controllo dell'integrità integro quando il numero specificato di controlli dell'integrità aggiunti a Controlli dell'integrità da monitorare sono integri. Tieni presente quanto segue:
  - Se specifichi un numero maggiore del numero di controlli dell'integrità riportato in Controlli dell'integrità da monitorare, Route 53 considera sempre questo controllo dell'integrità non integro.
  - Se specifichi 0, Route 53 considera sempre questo controllo dell'integrità integro.
- Segnala integro quando tutti i controlli dell'integrità sono integri (AND): Route 53 considera questo controllo dell'integrità integro solo quando tutti i controlli dell'integrità aggiunti a Controlli dell'integrità da monitorare sono integri.
- Segnala integro quando uno o più controlli dell'integrità sono integri (OR): Route 53 considera questo controllo dell'integrità integro quando almeno uno dei controlli dell'integrità aggiunto a Controlli dell'integrità da monitorare è integro.

Inverti lo stato del controllo dello stato di salute (solo la vecchia console)

Per invertire il controllo dello stato di salute sulla nuova console, vedi. Inversione dei controlli sanitari

Scegli se desideri che Route 53 inverta lo stato di un controllo dell'integrità. Se scegli questa opzione, Route 53 considera i controlli dell'integrità come non integri quando lo stato è integro e viceversa.

Disabilitato (solo la vecchia console)

Per disabilitare un controllo dello stato di salute sulla nuova console, vediDisabilitazione o attivazione dei controlli sanitari.

Fa sì che Route 53 interrompa l'esecuzione dei controlli dell'integrità. Quando si disabilita un controllo dell'integrità, Route 53 smette di aggregare lo stato dei controlli dell'integrità di riferimento.

Quando disabiliti un controllo dell'integrità, Route 53 considera lo stato del controllo dell'integrità sempre integro. Se hai configurato il failover DNS, Route 53 continua a instradare il traffico verso le risorse corrispondenti. Se desideri interrompere l'indirizzamento del traffico verso una risorsa, inverti il controllo dello stato.

> **Note**
>
> I costi per un controllo dell'integrità si applicano ancora quando il controllo dell'integrità è stato disabilitato.

Monitoraggio di un allarme CloudWatch

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Se desideri che questo controllo sanitario monitori lo stato di allarme di un CloudWatch allarme, specifica i seguenti valori:

- CloudWatch allarme

- Stato del controllo dell'integrità

CloudWatch allarme

Scegli l' CloudWatch allarme che desideri venga utilizzato da Route 53 per determinare se questo controllo sanitario è valido. L' CloudWatch allarme deve corrispondere Account AWS al controllo sanitario.

> **Note**
>
> Route 53 supporta CloudWatch allarmi con le seguenti funzionalità:
>
> - Parametri con risoluzione standard. I parametri ad alta risoluzione non sono supportati. Per ulteriori informazioni, consulta i parametri ad alta risoluzione nella Amazon CloudWatch User Guide.
> - Statistiche: `Average`, `Minimum`, `Maximum`, `Sum` e `SampleCount`. Le statistiche estese non sono supportate.
> - Route 53 non supporta gli allarmi "M di N" . Per ulteriori informazioni, consulta la sezione Valutazione di un allarme nella CloudWatch guida di Amazon.
>
> Route 53 non supporta gli allarmi che utilizzano la matematica metrica per interrogare più metriche. CloudWatch

Se desideri creare un allarme, completa la procedura seguente:

1. Scegli create (crea). La CloudWatch console viene visualizzata in una nuova scheda del browser.
2. Immetti i valori applicabili. Per ulteriori informazioni, consulta Creare o modificare un CloudWatch allarme nella Amazon CloudWatch User Guide.
3. Torna alla scheda del browser in cui compare la console Route 53.
4. Scegli il pulsante di aggiornamento accanto all'elenco degli CloudWatchavvisi.
5. Scegli il nuovo allarme dall'elenco.

> **Important**
>
> Se si modificano le impostazioni dell' CloudWatch allarme dopo aver creato un controllo dello stato di salute, è necessario aggiornare il controllo dello stato. Per

ulteriori informazioni, consulta Aggiornamento dei controlli sanitari quando modifichi le impostazioni CloudWatch degli allarmi (controlli sanitari che monitorano solo un CloudWatch allarme).

Stato del controllo dell'integrità

Scegli lo stato del controllo sanitario (integro, non integro o ultimo stato noto) quando CloudWatch i dati sono insufficienti per determinare lo stato dell'allarme che hai scelto per l'CloudWatchallarme. Se scegli di utilizzare l'ultimo stato noto, Route 53 utilizza lo stato del controllo di integrità dell'ultima volta che CloudWatch aveva dati sufficienti per determinare lo stato dell'allarme. Per i nuovi controlli dell'integrità che non hanno un ultimo stato noto, lo stato di default per il controllo dell'integrità è integro.

Il valore di Health check status fornisce uno stato temporaneo quando il flusso di dati per una CloudWatch metrica non è disponibile per un breve periodo. (Route 53 monitora i flussi di dati per le CloudWatch metriche, non lo stato dell'allarme corrispondente.) Se il parametro non sarà disponibile di frequente o per lunghi periodi (di durata superiore a poche ore), ti consigliamo di non utilizzare l'ultimo stato noto.

Old console

Se desideri che questo controllo sanitario monitori lo stato di allarme di un CloudWatch allarme, specifica i seguenti valori:

- CloudWatch allarme
- Stato del controllo dell'integrità
- Inverti stato del controllo dell'integrità
- Disabilitato

CloudWatch allarme

Scegli l' CloudWatch allarme che desideri venga utilizzato da Route 53 per determinare se questo controllo sanitario è valido. L' CloudWatch allarme deve corrispondere Account AWS al controllo sanitario.

> **Note**
>
> Route 53 supporta CloudWatch allarmi con le seguenti funzionalità:
>
> - Parametri con risoluzione standard. I parametri ad alta risoluzione non sono supportati. Per ulteriori informazioni, consulta i parametri ad alta risoluzione nella Amazon CloudWatch User Guide.
> - Statistiche: `Average`, `Minimum`, `Maximum`, `Sum` e `SampleCount`. Le statistiche estese non sono supportate.
> - Route 53 non supporta gli allarmi "M di N" . Per ulteriori informazioni, consulta la sezione Valutazione di un allarme nella CloudWatch guida di Amazon.
>
> Route 53 non supporta gli allarmi che utilizzano la matematica metrica per interrogare più metriche. CloudWatch

Se desideri creare un allarme, completa la procedura seguente:

1. Scegli create (crea). La CloudWatch console viene visualizzata in una nuova scheda del browser.
2. Immetti i valori applicabili. Per ulteriori informazioni, consulta Creare o modificare un CloudWatch allarme nella Amazon CloudWatch User Guide.
3. Torna alla scheda del browser in cui compare la console Route 53.
4. Scegli il pulsante di aggiornamento accanto all'elenco degli CloudWatchavvisi.
5. Scegli il nuovo allarme dall'elenco.

> **Important**
>
> Se si modificano le impostazioni dell' CloudWatch allarme dopo aver creato un controllo dello stato di salute, è necessario aggiornare il controllo dello stato. Per ulteriori informazioni, consulta Aggiornamento dei controlli sanitari quando modifichi le impostazioni CloudWatch degli allarmi (controlli sanitari che monitorano solo un CloudWatch allarme).

Stato del controllo dell'integrità

Scegli lo stato del controllo sanitario (integro, non integro o ultimo stato noto) quando CloudWatch i dati sono insufficienti per determinare lo stato dell'allarme che hai scelto per l'CloudWatchallarme. Se scegli di utilizzare l'ultimo stato noto, Route 53 utilizza lo stato del controllo di integrità dell'ultima volta che CloudWatch aveva dati sufficienti per determinare lo stato dell'allarme. Per i nuovi controlli dell'integrità che non hanno un ultimo stato noto, lo stato di default per il controllo dell'integrità è integro.

Il valore di Health check status fornisce uno stato temporaneo quando il flusso di dati per una CloudWatch metrica non è disponibile per un breve periodo. (Route 53 monitora i flussi di dati per le CloudWatch metriche, non lo stato dell'allarme corrispondente.) Se il parametro non sarà disponibile di frequente o per lunghi periodi (di durata superiore a poche ore), ti consigliamo di non utilizzare l'ultimo stato noto.

Inverti lo stato del controllo di integrità (solo la vecchia console)

Per invertire il controllo dello stato di salute sulla nuova console, vedi. Inversione dei controlli sanitari

Scegli se desideri che Route 53 inverta lo stato di un controllo dell'integrità. Se scegli questa opzione, Route 53 considera i controlli dell'integrità come non integri quando lo stato è integro e viceversa.

Disabilitato (solo la vecchia console)

Per disabilitare un controllo dello stato di salute sulla nuova console, vediDisabilitazione o attivazione dei controlli sanitari.

Fa sì che Route 53 interrompa l'esecuzione dei controlli dell'integrità. Quando disabiliti un controllo dello stato, Route 53 interrompe il monitoraggio delle CloudWatch metriche corrispondenti.

Quando disabiliti un controllo dell'integrità, Route 53 considera lo stato del controllo dell'integrità sempre integro. Se hai configurato il failover DNS, Route 53 continua a instradare il traffico verso le risorse corrispondenti. Se desideri interrompere l'indirizzamento del traffico verso una risorsa, inverti il controllo dello stato.

> **Note**
>
> I costi per un controllo dell'integrità si applicano ancora quando il controllo dell'integrità è stato disabilitato.

Configurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint))

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

- Nuova console
- Vecchia console

New console

- Intervallo di richiesta
- Soglia di errore
- Corrispondenza tra
- Stringhe di ricerca
- Grafici di latenza
- Abilita SNI
- Host name (Nome host)

Intervallo richiesta

Il numero di secondi tra il momento in cui ciascuno strumento di controllo dell'integrità di Route 53 riceve una risposta dal tuo endpoint e l'orario in cui invia la richiesta di controllo dell'integrità successiva. Se scegli un intervallo di 30 secondi, ciascuno degli strumenti di controllo dell'integrità di Route 53 nei data center in tutto il mondo invia la tua richiesta di controllo dell'integrità di un endpoint ogni 30 secondi. In media, il tuo endpoint riceverà una richiesta di controllo dell'integrità ogni due secondi. Se scegli un intervallo di 10 secondi, l'endpoint riceverà una richiesta più di una volta al secondo.

Gli strumenti di controllo dell'integrità di Route 53 in diversi data center non sono coordinati tra loro, perciò potrai talvolta vedere diverse richieste al secondo indipendentemente dall'intervallo di tempo scelto, seguito da alcuni secondi, senza controlli dell'integrità.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di Request interval (Intervallo di richiesta).

> **Note**
>
> Se scegli Fast (10 seconds) (Veloce (10 secondi)) per il valore di Request interval (Intervallo di richiesta), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Soglia di errore

Il numero di controlli dell'integrità consecutivi che un endpoint deve superare o non superare affinché Route 53 modifichi lo stato attuale dell'endpoint da integro a non integro o viceversa. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Stringa corrispondente (solo HTTP e HTTPS)

Se desideri che Route 53 determini lo stato di un endpoint inviando una richiesta HTTP o HTTPS all'endpoint e cecando il corpo della risposta per una stringa specificata. Se il corpo della risposta contiene il valore specificato in Stringa di ricerca, Route 53 considera l'endpoint integro. In caso contrario, oppure se l'endpoint non risponde, Route 53 considera l'endpoint non integro. La stringa di ricerca deve essere visualizzata in modo completo entro i primi 5.120 byte del corpo della risposta.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di String matching (Corrispondenza stringa).

> **Note**
>
> Se scegli Yes (Sì) per il valore del String matching (Corrispondenza stringa), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Come gli strumenti di controllo dell'integrità gestiscono una risposta compressa

Se l'endpoint è un server Web che restituisce una risposta compressa, lo strumento di controllo dell'integrità di Route 53 decomprimerà la risposta prima di verificare la stringa di ricerca specificata solo se il server Web ha compresso la risposta utilizzando un algoritmo di compressione supportato dagli strumenti di controllo dell'integrità. Gli strumenti di controllo dell'integrità supportano i seguenti algoritmi di compressione:

- Gzip
- Deflate

Se la risposta viene compressa utilizzando un altro algoritmo, lo strumento di controllo dell'integrità non può decomprimere la risposta prima di cercare la stringa. In questo caso, la ricerca avrà quasi sempre esito negativo e Route 53 considererà l'endpoint non integro.

Cerca stringa (solo quando "String matching" (Corrispondenza stringa) è abilitato)

La stringa che desideri che Route 53 cerchi nel corpo della risposta dal tuo endpoint. La lunghezza massima è 255 caratteri.

Route 53 tiene conto delle maiuscole e minuscole per Stringa di ricerca nel corpo della risposta.

Grafici di latenza

Scegli se vuoi che Route 53 misuri la latenza tra gli addetti al controllo dello stato di salute in più AWS regioni e il tuo endpoint. Se scegli questa opzione, i grafici CloudWatch della latenza vengono visualizzati nella scheda Latenza della pagina Health checks nella console Route 53. Se gli strumenti di controllo dell'integrità di Route 53 non possono connettersi all'endpoint, Route 53 non potrà visualizzare i grafici di latenza per quell'endpoint.

Dopo aver creato un controllo dell'integrità, non puoi modificare il valore di Latency measurements (Misurazioni di latenza).

> **Note**
>
> Se configuri Route 53 per misurare la latenza tra gli strumenti di controllo dell'integrità e il tuo endpoint, si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Abilita SNI (solo HTTPS)

Puoi indicare se desideri che Route 53 invii il nome host all'endpoint nel messaggio `client_hello` durante la negoziazione TLS. Ciò consente all'endpoint di rispondere alla richiesta HTTPS con il certificato SSL/TLS applicabile.

Alcuni endpoint richiedono che le richieste HTTPS includano il nome host nel messaggio client_hello. Se non abiliti SNI, lo stato del controllo di integrità potrebbe mostrare un errore. Il messaggio di errore dipenderà dalla configurazione del server per rispondere alla richiesta che non contiene informazioni SNI. Un controllo sanitario può avere lo stato di fallimento anche per altri motivi. Se SNI è abilitato e ottieni ancora l'errore, controlla la configurazione SSL/TLS sul tuo endpoint e conferma che il tuo certificato sia valido.

Si notino i requisiti seguenti:

- L'endpoint deve supportare SNI.
- Il certificato SSL/TLS sul tuo endpoint include un nome di dominio nel campo `Common Name` e possibilmente più nomi nel campo `Subject Alternative Names`. Uno dei nomi di dominio nel certificato deve corrispondere al valore che specifichi per Host name (Nome host).

Regioni dello strumento di controllo dell'integrità

Scegli se desideri che Route 53 controlli l'integrità dell'endpoint utilizzando gli strumenti di controllo dell'integrità nelle regioni consigliate o utilizzando strumenti di controllo dell'integrità in regioni da te specificate.

Se aggiorni un controllo dell'integrità per rimuovere una regione in cui si stanno eseguendo controlli dell'integrità, Route 53 continuerà a eseguire i controlli da quella regione per un massimo di un'ora. In questo modo è possibile assicurare che alcuni strumenti di controllo dell'integrità controllino sempre l'endpoint (ad esempio, se si sostituiscono tre regioni con quattro regioni diverse).

Se scegli Customize (Personalizza), scegli la x per una regione per rimuoverla. Fai clic sullo spazio in basso per riaggiungere una regione all'elenco. Devi specificare almeno tre regioni.

Nome host (solo "Specify endpoint by IP address" (Specifica endpoint in base all'indirizzo IP), solo protocolli HTTP e HTTPS)

Il valore che desideri che Route 53 passi nell'intestazione `Host` nei controlli dell'integrità HTTP e HTTPS. Questo è in genere il nome DNS completo del sito Web su cui desideri che

Route 53 esegua controlli dell'integrità. Quando Route 53 controlla lo stato di un endpoint, ecco come costruisce l'intestazione `Host`:

- Se specifichi un valore **`80`** per Porta e HTTP per Protocollo, Route 53 invia all'endpoint una intestazione `Host` che contiene il valore di Nome host.
- Se si specifica un valore **`443`** per Port e HTdTPS per Protocol, Route 53 passa all'endpoint un'**`Host`**intestazione che contiene il valore di Host name.
- Se si specifica un altro valore per Port e HTTP o HTTPS per Protocol, Route 53 passa all'endpoint un'**`Host`**intestazione che contiene il valore:. ***`Host name`*** *`Port`*

Se scegli di specificare l'endpoint in base all'indirizzo IP e non specifichi un valore per Nome host, Route 53 sostituisce il valore di Indirizzo IP nell'intestazione `Host` in ciascuno dei casi precedenti.

Old console

Se scegli l'opzione che consente di monitorare un endpoint, puoi anche specificare le impostazioni seguenti:

- Intervallo di richiesta
- Soglia di errore
- Corrispondenza tra
- Stringa di ricerca
- Grafico della latenza
- Abilita SNI
- Regioni Health checker
- Inverti stato del controllo dell'integrità
- Disabilitato

Intervallo richiesta

Il numero di secondi tra il momento in cui ciascuno strumento di controllo dell'integrità di Route 53 riceve una risposta dal tuo endpoint e l'orario in cui invia la richiesta di controllo dell'integrità successiva. Se scegli un intervallo di 30 secondi, ciascuno degli strumenti di controllo dell'integrità di Route 53 nei data center in tutto il mondo invia la tua richiesta di controllo dell'integrità di un endpoint ogni 30 secondi. In media, il tuo endpoint riceverà una

richiesta di controllo dell'integrità ogni due secondi. Se scegli un intervallo di 10 secondi, l'endpoint riceverà una richiesta più di una volta al secondo.

Gli strumenti di controllo dell'integrità di Route 53 in diversi data center non sono coordinati tra loro, perciò potrai talvolta vedere diverse richieste al secondo indipendentemente dall'intervallo di tempo scelto, seguito da alcuni secondi, senza controlli dell'integrità.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di Request interval (Intervallo di richiesta).

> **Note**
>
> Se scegli Fast (10 seconds) (Veloce (10 secondi)) per il valore di Request interval (Intervallo di richiesta), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Soglia di errore

Il numero di controlli dell'integrità consecutivi che un endpoint deve superare o non superare affinché Route 53 modifichi lo stato attuale dell'endpoint da integro a non integro o viceversa. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Stringa corrispondente (solo HTTP e HTTPS)

Se desideri che Route 53 determini lo stato di un endpoint inviando una richiesta HTTP o HTTPS all'endpoint e cecando il corpo della risposta per una stringa specificata. Se il corpo della risposta contiene il valore specificato in Stringa di ricerca, Route 53 considera l'endpoint integro. In caso contrario, oppure se l'endpoint non risponde, Route 53 considera l'endpoint non integro. La stringa di ricerca deve essere visualizzata in modo completo entro i primi 5.120 byte del corpo della risposta.

Dopo aver creato un controllo dell'integrità, non è possibile modificare il valore di String matching (Corrispondenza stringa).

> **Note**
>
> Se scegli Yes (Sì) per il valore del String matching (Corrispondenza stringa), si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Come gli strumenti di controllo dell'integrità gestiscono una risposta compressa

Se l'endpoint è un server Web che restituisce una risposta compressa, lo strumento di controllo dell'integrità di Route 53 decomprimerà la risposta prima di verificare la stringa di ricerca specificata solo se il server Web ha compresso la risposta utilizzando un algoritmo di compressione supportato dagli strumenti di controllo dell'integrità. Gli strumenti di controllo dell'integrità supportano i seguenti algoritmi di compressione:

- Gzip
- Deflate

Se la risposta viene compressa utilizzando un altro algoritmo, lo strumento di controllo dell'integrità non può decomprimere la risposta prima di cercare la stringa. In questo caso, la ricerca avrà quasi sempre esito negativo e Route 53 considererà l'endpoint non integro.

Cerca stringa (solo quando "String matching" (Corrispondenza stringa) è abilitato)

La stringa che desideri che Route 53 cerchi nel corpo della risposta dal tuo endpoint. La lunghezza massima è 255 caratteri.

Route 53 tiene conto delle maiuscole e minuscole per Stringa di ricerca nel corpo della risposta.

Grafici di latenza

Scegli se desideri che Route 53 misuri la latenza tra i controllori sanitari di più AWS regioni e il tuo endpoint. Se scegli questa opzione, i grafici CloudWatch della latenza vengono visualizzati nella scheda Latenza della pagina Health checks nella console Route 53. Se gli strumenti di controllo dell'integrità di Route 53 non possono connettersi all'endpoint, Route 53 non potrà visualizzare i grafici di latenza per quell'endpoint.

Dopo aver creato un controllo dell'integrità, non puoi modificare il valore di Latency measurements (Misurazioni di latenza).

> **Note**
>
> Se configuri Route 53 per misurare la latenza tra gli strumenti di controllo dell'integrità e il tuo endpoint, si applica un costo aggiuntivo. Per ulteriori informazioni, consulta Prezzi di Route 53.

Abilita SNI (solo HTTPS)

Puoi indicare se desideri che Route 53 invii il nome host all'endpoint nel messaggio `client_hello` durante la negoziazione TLS. Ciò consente all'endpoint di rispondere alla richiesta HTTPS con il certificato SSL/TLS applicabile.

Alcuni endpoint richiedono che le richieste HTTPS includano il nome host nel messaggio `client_hello`. Se non abiliti SNI, lo stato del controllo di integrità potrebbe mostrare un errore. Il messaggio di errore dipende dalla configurazione del server per rispondere alla richiesta che non contiene informazioni SNI. Un controllo sanitario può avere lo stato di fallimento anche per altri motivi. Se SNI è abilitato e ottieni ancora l'errore, controlla la configurazione SSL/TLS sul tuo endpoint e conferma che il tuo certificato sia valido.

Si notino i requisiti seguenti:

- L'endpoint deve supportare SNI.
- Il certificato SSL/TLS sul tuo endpoint include un nome di dominio nel campo `Common Name` e possibilmente più nomi nel campo `Subject Alternative Names`. Uno dei nomi di dominio nel certificato deve corrispondere al valore che specifichi per Host name (Nome host).

Regioni dello strumento di controllo dell'integrità

Scegli se desideri che Route 53 controlli l'integrità dell'endpoint utilizzando gli strumenti di controllo dell'integrità nelle regioni consigliate o utilizzando strumenti di controllo dell'integrità in regioni da te specificate.

Se aggiorni un controllo dell'integrità per rimuovere una regione in cui si stanno eseguendo controlli dell'integrità, Route 53 continuerà a eseguire i controlli da quella regione per un massimo di un'ora. In questo modo è possibile assicurare che alcuni strumenti di controllo dell'integrità controllino sempre l'endpoint (ad esempio, se si sostituiscono tre regioni con quattro regioni diverse).

Se scegli Customize (Personalizza), scegli la x per una regione per rimuoverla. Fai clic sullo spazio in basso per riaggiungere una regione all'elenco. Devi specificare almeno tre regioni.

Inverti lo stato del controllo di integrità (solo la vecchia console)

Per invertire il controllo dello stato di salute sulla nuova console, vedi. Inversione dei controlli sanitari

Scegli se desideri che Route 53 inverta lo stato di un controllo dell'integrità. Se scegli questa opzione, Route 53 considera un controllo sanitario non integro quando lo stato è integro e viceversa. Ad esempio, potresti volere che Route 53 consideri un controllo dell'integrità non integro se configuri la corrispondenza della stringa e l'endpoint restituisce un valore specificato.

Disabilitato (solo vecchia console)

Per disabilitare un controllo dello stato di salute sulla nuova console, vediDisabilitazione o attivazione dei controlli sanitari.

Fa sì che Route 53 interrompa l'esecuzione dei controlli dell'integrità. Quando disabiliti un controllo dell'integrità, Route 53 smette di cercare di stabilire una connessione TCP con l'endpoint.

Quando disabiliti un controllo dell'integrità, Route 53 considera lo stato del controllo dell'integrità sempre integro. Se hai configurato il failover DNS, Route 53 continua a instradare il traffico verso le risorse corrispondenti. Se desideri interrompere l'indirizzamento del traffico verso una risorsa, inverti il controllo dello stato.

> **Note**
>
> I costi per un controllo dell'integrità si applicano ancora quando il controllo dell'integrità è stato disabilitato.

Ricevere una notifica quando il controllo dell'integrità ha esito negativo

Utilizza le seguenti opzioni per configurare le notifiche via e-mail quando un controllo dell'integrità ha esito negativo:

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Crea allarme (solo quando si creano controlli dell'integrità)

Specificate se desiderate creare un allarme predefinito CloudWatch . Se scegli Sì, ti CloudWatch invia una notifica Amazon SNS quando lo stato di questo endpoint diventa non integro e Route 53 considera l'endpoint non integro per un minuto.

> **Note**
>
> Se desideri CloudWatch inviarti un'altra notifica Amazon SNS quando lo stato torna a integro, puoi creare un altro allarme dopo aver creato il controllo dello stato. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi Amazon nella Amazon CloudWatch User Guide.

Se desideri creare un allarme per un controllo dell'integrità esistente o ricevere notifiche quando Route 53 considera l'endpoint non integro per più o meno di un minuto (il valore di default), seleziona No e aggiungi un allarme dopo aver creato il controllo dell'integrità. Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

Invia notifica a (solo durante la creazione di un allarme)

Specificate se desiderate CloudWatch inviare notifiche a un argomento Amazon SNS esistente o a uno nuovo:

- Argomento SNS esistente: seleziona il nome dell'argomento dall'elenco. L'argomento deve trovarsi nella regione Stati Uniti orientali (Virginia settentrionale).
- Nuovo argomento SNS: inserisci un nome per l'argomento in Nome argomento, quindi immetti l'indirizzo e-mail a cui desideri inviare notifiche nel campo Destinatari. Separa più indirizzo con virgole (,), punti e virgola (;), o spazi.

  Route 53 creerà l'argomento nella regione Stati Uniti orientali (Virginia settentrionale).

Nome argomento (solo durante la creazione di un nuovo argomento SNS)

Se hai specificato New SNS Topic (Nuovo argomento SNS), inserisci il nome del nuovo argomento.

Indirizzi e-mail destinatari (solo durante la creazione di un nuovo argomento SNS)

Se hai specificato New SNS topic (Nuovo argomento SNS), immetti l'indirizzo e-mail a cui desideri inviare notifiche. Separa più nomi con virgole (,), punti e virgola (;), o spazi.

Valori visualizzati da Amazon Route 53 durante la creazione di un controllo dell'integrità

Nella pagina Create Health Check (Crea controllo dell'integrità) sono mostrati i seguenti valori in base ai valori inseriti:

URL

Può essere l'URL completo (per i controlli dell'integrità HTTP o HTTPS) o l'indirizzo IP e la porta (per i controlli dell'integrità TCP) a cui Route 53 invierà richieste quando si eseguono controlli dell'integrità.

Tipo di controllo dell'integrità

Basic (Base) o Basic + additional options (Base + opzioni aggiuntive) in base alle impostazioni che hai specificato per questo controllo dell'integrità. Per informazioni sui prezzi per le opzioni aggiuntive, consulta Prezzi di Route 53.

Aggiornamento dei controlli sanitari quando modifichi le impostazioni CloudWatch degli allarmi (controlli sanitari che monitorano solo un CloudWatch allarme)

Se si crea un controllo dello stato di Route 53 che monitora il flusso di dati alla ricerca di un CloudWatch allarme e poi si aggiornano le impostazioni dell' CloudWatch allarme, Route 53 non aggiorna automaticamente le impostazioni di allarme durante il controllo dello stato. Se desideri che il controllo dell'integrità inizi a usare le nuove impostazioni di allarme, devi aggiornare il controllo dell'integrità.

> **Note**
>
> Per aggiornare un controllo dell'integrità a livello di codice, puoi utilizzare l'API `UpdateHealthCheck`. Basta specificare i valori correnti per `AlarmIdentifier` e `Region` Route 53 otterrà le impostazioni più recenti da CloudWatch. Per ulteriori informazioni, UpdateHealthCheckconsulta Amazon Route 53 API Reference.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per aggiornare un controllo sanitario con nuove impostazioni di CloudWatch allarme

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Seleziona l'ID collegato per il controllo sanitario che desideri aggiornare.
4. Scegli Modifica.

   Una nota spiega che l' CloudWatch allarme per il controllo sanitario è cambiato. Il campo Details (Dettagli) mostra le nuove impostazioni di allarme.
5. Seleziona Salva.

Old console

Per aggiornare un controllo sanitario con nuove impostazioni di CloudWatch allarme (console)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
3. Selezionare la casella di controllo il controllo dell'integrità che desideri aggiornare.
4. Scegli Edit health check (Modifica controllo dell'integrità).

   Una nota spiega che l' CloudWatch allarme per il controllo sanitario è cambiato. Il campo Details (Dettagli) mostra le nuove impostazioni di allarme.

5. Seleziona Salva.

Disabilitazione o attivazione dei controlli sanitari

La disabilitazione di un controllo dello stato impedisce a Route 53 di eseguire i controlli sanitari. Quando si disabilita un controllo dell'integrità, Route 53 smette di aggregare lo stato dei controlli dell'integrità di riferimento. Quando disabiliti un controllo dell'integrità, Route 53 considera lo stato del controllo dell'integrità sempre integro. Se hai configurato il failover DNS, Route 53 continua a instradare il traffico verso le risorse corrispondenti.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Puoi disabilitare o abilitare un controllo dello stato sulla vecchia console quando crei o modifichi il controllo. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.

Per disabilitare i controlli di integrità sulla nuova console, eseguire la procedura seguente.

Per disabilitare o abilitare un controllo dello stato (solo nuova console)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Nella colonna Azioni, seleziona i tre punti, quindi Disabilita o Abilita.

   In alternativa, seleziona l'ID collegato del controllo sanitario che desideri disabilitare o abilitare.
4. Nella tabella Configurazione, il campo Stato specifica se il controllo dello stato è abilitato o disabilitato.
5. Scegli Disabilita o Abilita per disabilitare o abilitare il controllo sanitario.

Inversione dei controlli sanitari

Se si inverte un controllo dello stato di salute, Route 53 considera non corretto il controllo dello stato di salute e viceversa.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Puoi invertire un controllo dello stato sulla vecchia console quando crei o modifichi il controllo dello stato. Per ulteriori informazioni, consulta Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.

Per invertire i controlli di integrità sulla nuova console, effettuate la seguente procedura.

Per invertire un controllo di integrità (solo nuova console)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Nella colonna Azioni, seleziona i tre punti e poi Inverti.

   Oppure, seleziona l'ID collegato del controllo sanitario che desideri invertire.
4. Nella tabella di configurazione, il campo Invertito specifica se il controllo dello stato è invertito (Sì) o meno (No).
5. Scegli Inverti per invertire il controllo dello stato di salute.

   Se desideri annullare lo stato invertito e il campo Invertito è Sì, scegli nuovamente Inverti.

Eliminazione di controlli dell'integrità

Per disabilitare i controlli sanitari, effettuate la seguente procedura.

> **Note**
>
> Se utilizzi AWS Cloud Map e hai configurato AWS Cloud Map per creare un controllo dello stato di Route 53 quando registri un'istanza, non puoi utilizzare la console Route 53 per

eliminare il controllo dello stato. Il controllo dell'integrità viene eliminato automaticamente quando si annulla la registrazione dell'istanza. Potrebbe verificarsi un ritardo di diverse ore prima che il controllo dell'integrità non venga più visualizzato nella console Route 53.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per eliminare un controllo sanitario

1. In caso di eliminazione di controlli dell'integrità associati a record, eseguire le attività consigliate in Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione, scegli Health checks.
4. Seleziona l'ID collegato del controllo sanitario che desideri eliminare.
5. Scegli Elimina.
6. Entra **`confirm`** nella casella di testo e quindi scegli Elimina.

Old console

Per eliminare un controllo dell'integrità (console)

1. In caso di eliminazione di controlli dell'integrità associati a record, eseguire le attività consigliate in Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS.
2. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
3. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
4. Nel riquadro di destra, seleziona il controllo dell'integrità che desideri eliminare.
5. Scegli Delete Health Check (Elimina controllo dell'integrità).
6. Seleziona Yes, Delete (Sì, elimina) per confermare.

Aggiornamento o eliminazione di controlli dell'integrità quando è configurato il failover DNS

Quando desideri aggiornare o eliminare controlli dell'integrità associati a record, oppure se desideri modificare i record che hanno controlli dell'integrità associati, devi valutare il modo in cui le modifiche interessano il routing delle query DNS e la tua configurazione di failover DNS.

> **Important**
>
> Route 53 non impedisce di eliminare un controllo dell'integrità anche se il controllo è associato a uno o più record. Se elimini un controllo dell'integrità e non aggiorni i record associati, lo stato futuro del controllo dell'integrità non può essere previsto e potrebbe cambiare. Questo influenzerà il routing delle query DNS per la tua configurazione di failover DNS.

Per aggiornare o eliminare controlli dell'integrità che sono già associati a record, ti consigliamo di eseguire le attività seguenti:

1. Identificare i record che sono associati ai controlli dell'integrità. Per identificare i record associati a un controllo dell'integrità, devi procedere in uno dei seguenti modi:

- Rivedi i record in ciascuna zona ospitata utilizzando la console di Route 53. Per ulteriori informazioni, consulta Elencazione di record.
- Esegui l'operazione API `ListResourceRecordSets` in ciascuna azione zona ospitata ed esamina la risposta. Per ulteriori informazioni, ListResourceRecordSetsconsulta Amazon Route 53 API Reference.

2. Valuta la modifica del comportamento derivante dall'aggiornamento o dall'eliminazione di controlli dell'integrità o dall'aggiornamento di record. In base a tale valutazione, determina quale modifica attuare.

   Per ulteriori informazioni, consulta Cosa accade se si omettono i controlli dell'integrità?.

3. Modifica i controlli dell'integrità e i record come applicabile. Per ulteriori informazioni, consulta i seguenti argomenti:

   - Creazione e aggiornamento di controlli dell'integrità
   - Modifica di record

4. Elimina eventuali controlli dell'integrità che non utilizzi più. Per ulteriori informazioni, consulta Eliminazione di controlli dell'integrità.

Configurazione di regole di router e firewall per i controlli dell'integrità di Amazon Route 53

Quando Route 53 controlla lo stato di un endpoint, invia una richiesta HTTP, HTTPS o TCP all'indirizzo IP e alla porta specificati quando è stato creato il controllo dell'integrità. Affinché un controllo dell'integrità abbia esito positivo, le regole di router e firewall devono consentire il traffico in entrata dagli indirizzi IP utilizzati dagli strumenti di controllo dell'integrità di Route 53.

Per l'elenco aggiornato degli indirizzi IP per i controllori dello stato di Route 53, per i name server Route 53 e per altri AWS servizi, consultaIntervalli di indirizzi IP di server Amazon Route 53.

In Amazon EC2, i gruppi di sicurezza fungono da firewall. Per ulteriori informazioni, consulta i gruppi di EC2 sicurezza Amazon nella Amazon EC2 User Guide. Per configurare i gruppi di sicurezza in modo da consentire i controlli di integrità di Route 53, puoi consentire il traffico in entrata da ogni intervallo di indirizzi IP oppure puoi utilizzare un elenco di prefissi AWS gestiti.

Per utilizzare l'elenco dei prefissi AWS-managed, modifica il gruppo di sicurezza per consentire il traffico in entrata da `com.amazonaws.<region>.route53-healthchecks` dove si `<region>`

trova la Regione AWS tua EC2 istanza o risorsa Amazon. Se utilizzi i controlli di integrità di Route 53 per controllare gli IPv6 endpoint, dovresti consentire anche il traffico in entrata da. `com.amazonaws.<region>.ipv6.route53-healthchecks`

Per ulteriori informazioni sugli elenchi di prefissi AWS-managed, consulta Work with AWS-managed prefix lists nella Amazon VPC User Guide.

> **Important**
>
> Quando aggiungi indirizzi IP a un elenco di indirizzi IP consentiti, aggiungi tutti gli indirizzi IP dell'intervallo CIDR per ogni AWS regione specificata al momento della creazione dei controlli di integrità, oltre all'intervallo CIDR globale. È possibile che le richieste di controllo dell'integrità provengano da un solo indirizzo IP in una regione. Tuttavia, quell'indirizzo IP può variare in qualsiasi momento a un altro indirizzo IP per quella regione.
> Se desideri essere certo di includere sia gli indirizzi IP dello strumento di controllo dell'integrità corrente che quelli meno recenti, aggiungi gli intervalli di indirizzi IP ALL /26 e /18 all'elenco di valori consentiti. Per un elenco completo, consulta Intervalli di indirizzi IP AWS nella Riferimenti generali di AWS.
> Quando aggiungi l'elenco dei prefissi AWS-managed al gruppo di sicurezza in entrata, vengono aggiunti automaticamente tutti gli intervalli necessari.

Configurazione di un failover DNS

Quando si dispone di più di una risorsa che esegue la stessa funzione, ad esempio più di un server HTTP o un server di posta, puoi configurare Amazon Route 53 per controllare l'integrità delle tue risorse e rispondere alle query DNS utilizzando solo le risorse integre. Supponiamo ad esempio che il tuo sito Web, esempio.com, sia ospitato su sei server, distribuiti a due a due in tre data center situati in diverse zone del mondo. È possibile configurare Route 53 per controllare l'integrità dei server e rispondere alle query DNS per esempio.com utilizzando solo i server che sono attualmente integri.

Route 53 può controllare l'integrità delle risorse in configurazioni semplici e complesse:

- Nelle configurazioni semplici crei un gruppo di record il cui nome e tipo sono identici, ad esempio un gruppo di record ponderati con un tipo A per esempio.com. Quindi configura Route 53 perché controlli l'integrità delle risorse corrispondenti. Route 53 risponde alle query DNS in base all'integrità delle risorse. Per ulteriori informazioni, consulta Funzionamento dei controlli dell'integrità in configurazioni semplici di Amazon Route 53.

- Nelle configurazioni più complesse crei un albero di record che instradano il traffico in base a più criteri. Se ad esempio il tuo criterio più importante è la latenza per gli utenti, puoi utilizzare i record alias di latenza per instradare il traffico verso la regione che offre la latenza migliore. I record alias di latenza possono avere record ponderati in ciascuna regione come destinazione alias. I record ponderati potrebbero indirizzare il traffico verso EC2 le istanze in base al tipo di istanza. Come nel caso delle configurazioni semplici, puoi configurare Route 53 in modo che instradi il traffico in base all'integrità delle tue risorse. Per ulteriori informazioni, consulta Funzionamento dei controlli dell'integrità in configurazioni complesse di Amazon Route 53.

Argomenti

Elenco di attività per la configurazione del failover DNS

Per utilizzare Route 53 per configurare un failover DNS, completa le seguenti operazioni:

1. Disegna un diagramma ad albero completo della tua configurazione e indica quale tipo di record stai creando (alias ponderato, failover, latenza e così via) per ciascun nodo. In cima all'albero inserisci i record per il nome di dominio, ad esempio esempio.com, che gli utenti utilizzeranno per accedere al tuo sito o alla tua applicazione Web.

   I tipi di record che appaiono nel diagramma ad albero dipendono dalla complessità della configurazione:

   - Nel caso di una configurazione semplice, o il diagramma non includerà alcun record alias o i record alias instraderanno direttamente il traffico verso una risorsa (ad esempio un load balancer ELB) anziché a un altro record di Route 53. Per ulteriori informazioni, consulta Funzionamento dei controlli dell'integrità in configurazioni semplici di Amazon Route 53.

- In una configurazione complessa, il diagramma includerà una combinazione di record alias (ad esempio alias ponderati e alias di failover) e non alias in una struttura multi-livello come negli esempi nell'argomento Funzionamento dei controlli dell'integrità in configurazioni complesse di Amazon Route 53.

> **Note**
>
> Per creare in modo rapido e semplice record per configurazioni di routing complesse e associare i record ai controlli dell'integrità, puoi usare il l'editor visivo del flusso di traffico e salvare la configurazione come una policy di traffico. Puoi quindi associare la policy di traffico a uno o più nomi di dominio (ad esempio esempio.com) o nomi di sottodominio (ad esempio www.esempio.com), nella stessa zona ospitata o in più zone ospitate. Inoltre, puoi eseguire il roll back degli aggiornamenti se la nuova configurazione non offre le prestazioni previste. Per ulteriori informazioni, consulta Utilizzo di Traffic Flow per instradare il traffico DNS.

Per ulteriori informazioni, consulta la seguente documentazione :

- Scegliere una policy di routing
- Scelta tra record alias e non alias

2. Crea controlli di integrità per le risorse per le quali non puoi creare record di alias, come i EC2 server Amazon e i server di posta elettronica in esecuzione nel tuo data center. Dovrai associare questi controlli dell'integrità con i tuoi record non alias.

   Per ulteriori informazioni, consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.

3. Se necessario, configura le regole di router e firewall in modo che Route 53 possa inviare richieste regolari agli endpoint specificati nei controlli dell'integrità. Per ulteriori informazioni, consulta Configurazione di regole di router e firewall per i controlli dell'integrità di Amazon Route 53.

4. Crea tutti i record non alias nel tuo diagramma e associa i controlli dell'integrità creati nella fase 2 ai record applicabili.

   Se stai configurando un failover DNS in una configurazione che non include alcun record alias, ignora le operazioni rimanenti.

5. Crea i record di alias che indirizzano il traffico verso AWS risorse, come i sistemi di bilanciamento del carico e le distribuzioni ELB. CloudFront Se desideri che, quando una risorsa non è integra, Route 53 provi con un altro ramo dell'albero, imposta il valore di Valuta integrità destinazione su Sì per ciascun record alias. (Evaluate Target Health non è supportato per alcune AWS risorse.)
6. Cominciando dalla parte inferiore del diagramma creato nella fase 1, crea i record alias che instradano il traffico verso i record creati nelle fasi 4 e 5. Se desideri che, quando tutti i record non alias in un ramo dell'albero non sono integri, Route 53 provi un altro ramo, imposta il valore di Valuta integrità destinazione su Sì per ciascun record alias.

   Ricorda che non puoi creare un record alias in grado di instradare il traffico su un altro record finché non hai creato l'altro record.

Funzionamento dei controlli dell'integrità in configurazioni semplici di Amazon Route 53

Quando disponi di due o più risorse che eseguono la stessa funzione, ad esempio due o più server Web per esempio.com, puoi utilizzare le seguenti caratteristiche di controllo dell'integrità per instradare il traffico verso le risorse integre:

Controlla lo stato delle EC2 istanze e di altre risorse (record non alias)

Se stai indirizzando il traffico verso risorse per le quali non puoi creare record di alias, come EC2 le istanze, crei un record e un controllo dello stato di salute per ogni risorsa. In seguito puoi associare ogni controllo dell'integrità al record applicabile. I controlli dell'integrità verificano regolarmente l'integrità delle risorse corrispondenti e Route 53 instrada il traffico soltanto verso le risorse che i controlli reputano integre.

Valuta lo stato di salute di una AWS risorsa (record di alias)

Se utilizzi record di alias per indirizzare il traffico verso AWS risorse selezionate, come i sistemi di bilanciamento del carico ELB, puoi configurare Route 53 per valutare lo stato della risorsa e indirizzare il traffico solo verso risorse integre. Quando configuri un record alias per valutare lo stato di una risorsa, non è necessario creare un controllo dell'integrità per la risorsa in questione.

Ecco una panoramica di come configurare Route 53 affinché controlli l'integrità delle tue risorse nelle configurazioni semplici:

1. Identifica le risorse che desideri siano monitorate da Route 53. Potresti ad esempio voler monitorare tutti i server HTTP che rispondono alle richieste di esempio.com.
2. Crei controlli di integrità per le risorse per le quali non puoi creare record di alias, come EC2 istanze o server nel tuo data center. Specifica come inviare le richieste di controllo dell'integrità alla risorsa: quale protocollo utilizzare (HTTP, HTTPS o TCP), quale indirizzo IP e porta utilizzare e, per i controlli dell'integrità HTTP/HTTPS, un percorso e un nome di dominio.

   > **Note**
   >
   > Se utilizzi risorse per le quali non puoi creare record alias, ad esempio sistemi di bilanciamento del carico ELB, non creare controlli dell'integrità per tali risorse.

   Una configurazione comune è la creazione di un controllo dell'integrità per ciascuna risorsa e l'utilizzo dello stesso indirizzo IP per l'endpoint di controllo dell'integrità come per la risorsa. Il controllo dell'integrità invia le richieste all'indirizzo IP specificato.

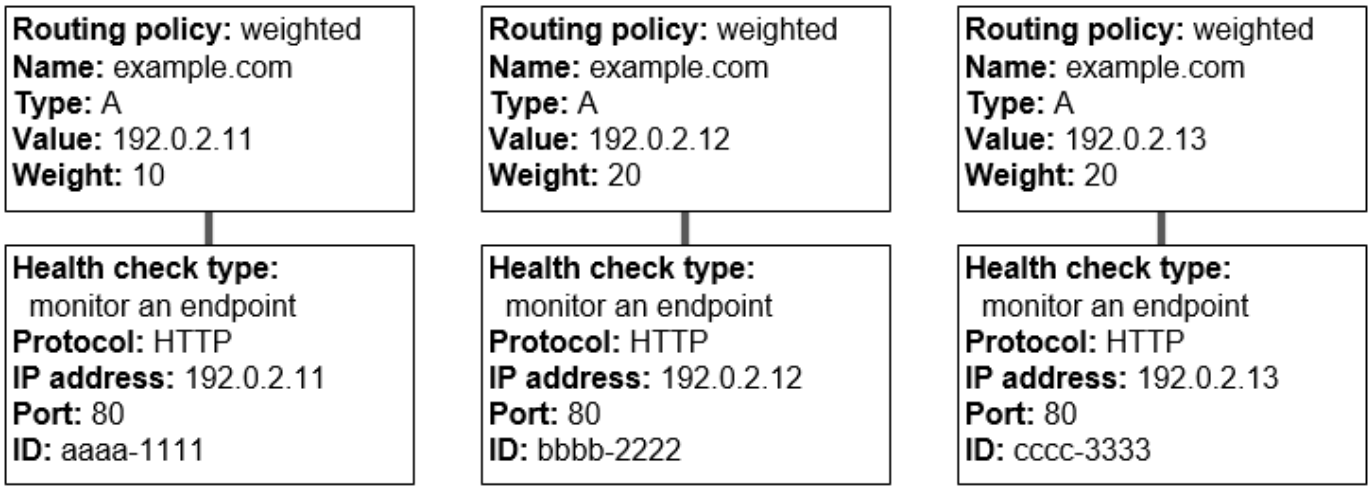
   > **Note**
   >
   > Route 53 non è in grado di verificare lo stato delle risorse il cui indirizzo IP è in intervalli locali, privati, non instradabili o multicast. Per ulteriori informazioni sugli indirizzi IP per i quali non è possibile creare controlli di integrità, consulta RFC 5735, Indirizzi per uso speciale e RFC 6598, Prefisso riservato IANA IPv4 per lo spazio di IPv4 indirizzi condiviso.

   Per ulteriori informazioni sulla creazione dei controlli dell'integrità, consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.
3. Potrebbe essere necessario configurare regole di router e firewall in modo che Route 53 possa inviare richieste regolari agli endpoint specificati nei controlli dell'integrità. Per ulteriori informazioni, consulta Configurazione di regole di router e firewall per i controlli dell'integrità di Amazon Route 53.
4. Crea un gruppo di record per le risorse, ad esempio un gruppo di record ponderati. Puoi combinare record alias e non alias, ma tutti devono avere lo stesso valore di Nome, Tipo e Policy di routing.

Il modo in cui configuri Route 53 per la verifica dello stato delle tue risorse varia a seconda che tu voglia creare record alias o record non alias:

- Record alias: specifica Sì per Valuta integrità destinazione.
- Record non alias: associa i controlli dell'integrità creati nella fase 2 ai record corrispondenti.

Al termine, la configurazione risulterà simile al diagramma seguente, il quale include solo record non alias.



Per informazioni sulla creazione di record utilizzando la console Route 53, consulta Creazione di record utilizzando la console Amazon Route 53.

5. Sei hai creato i controlli dell'integrità, Route 53 invia richieste periodiche all'endpoint per ciascun controllo dell'integrità e non esegue il controllo dell'integrità quando riceve una query DNS. In base alla risposte, Route 53 decide se l'endpoint è integro e utilizza queste informazioni per determinare come rispondere alle query. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

   Route 53 non controlla l'integrità della risorsa specificata nel record, ad esempio l'indirizzo IP specificato in un record A per esempio.com. Quando associ un controllo dell'integrità a un record, Route 53 inizia a controllare l'integrità dell'endpoint specificato nel controllo dell'integrità. Puoi anche configurare Route 53 per monitorare lo stato di altri controlli sanitari o monitorare i flussi di dati in caso di allarmi. CloudWatch Per ulteriori informazioni, consulta Tipi di controlli dell'integrità di Amazon Route 53.

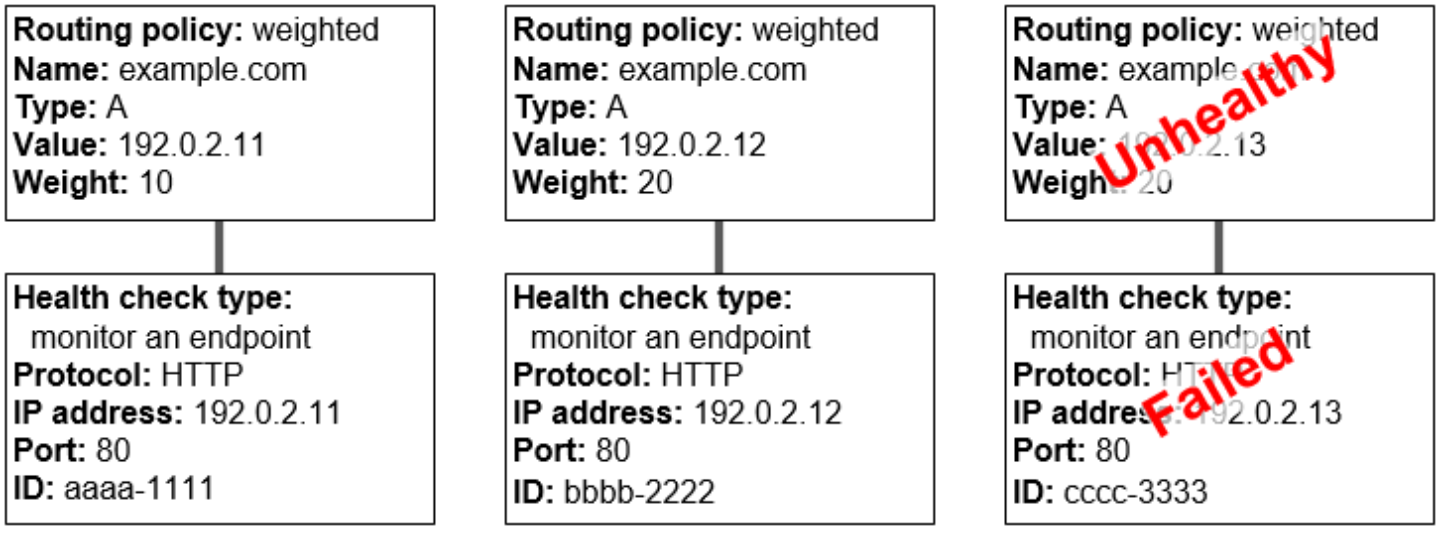
Ecco cosa succede quando Route 53 riceve una query per esempio.com:

1. Route 53 sceglie un record in base alla policy di routing. In questo caso, sceglie un record in base al peso.
2. Determina l'attuale stato del record selezionato controllando lo stato del controllo dell'integrità per quel record.
3. Se il record selezionato non è integro, Route 53 ne seleziona un altro. Questa volta, il record non integro non è preso in considerazione.

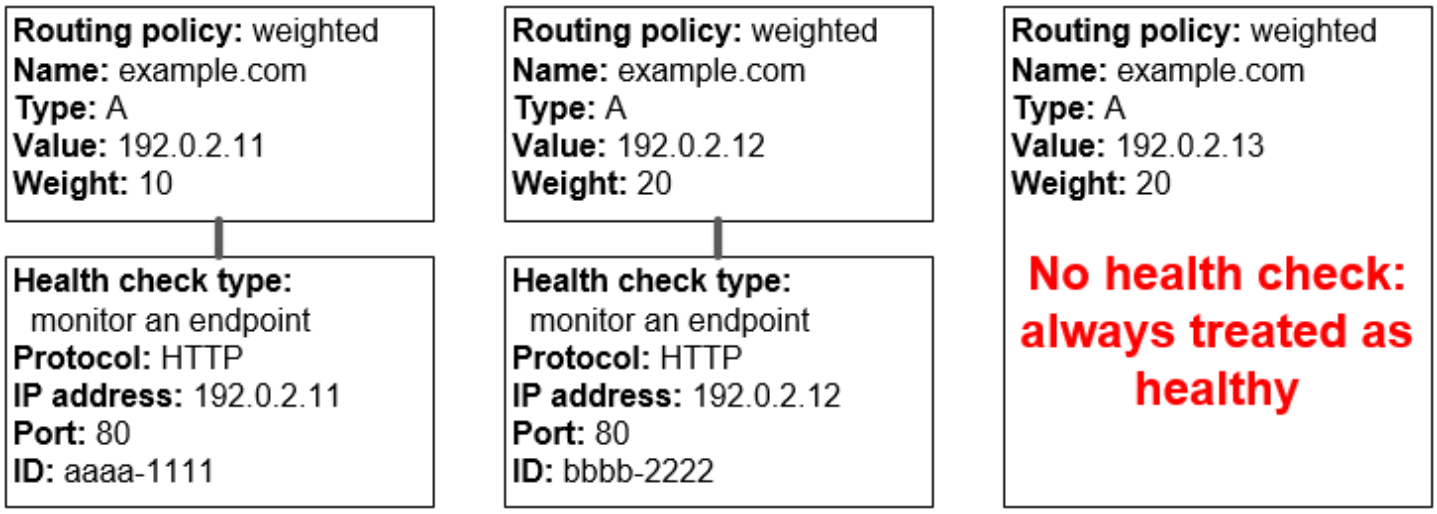
   Per ulteriori informazioni, consulta Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità.
4. Quando trova un record integro, Route 53 risponde alla query con il valore applicabile, ad esempio l'indirizzo IP in un record A.

L'esempio seguente mostra un gruppo di record ponderati in cui il terzo record non è integro. Inizialmente Route 53 seleziona un record in base al peso di tutti e tre i record. Se seleziona il record non integro la prima volta, Route 53 seleziona un altro record, ma questa volta viene omesso il peso del terzo record dal calcolo:

- Quando Route 53 inizialmente seleziona tra tutte e tre i record, risponde alle richieste utilizzando il primo record circa il 20% del tempo, 10/(10+20+20).
- Quando Route 53 determina che il terzo record non è integro, risponde alle richieste utilizzando il primo record circa il 33% del tempo, 10/(10+20).



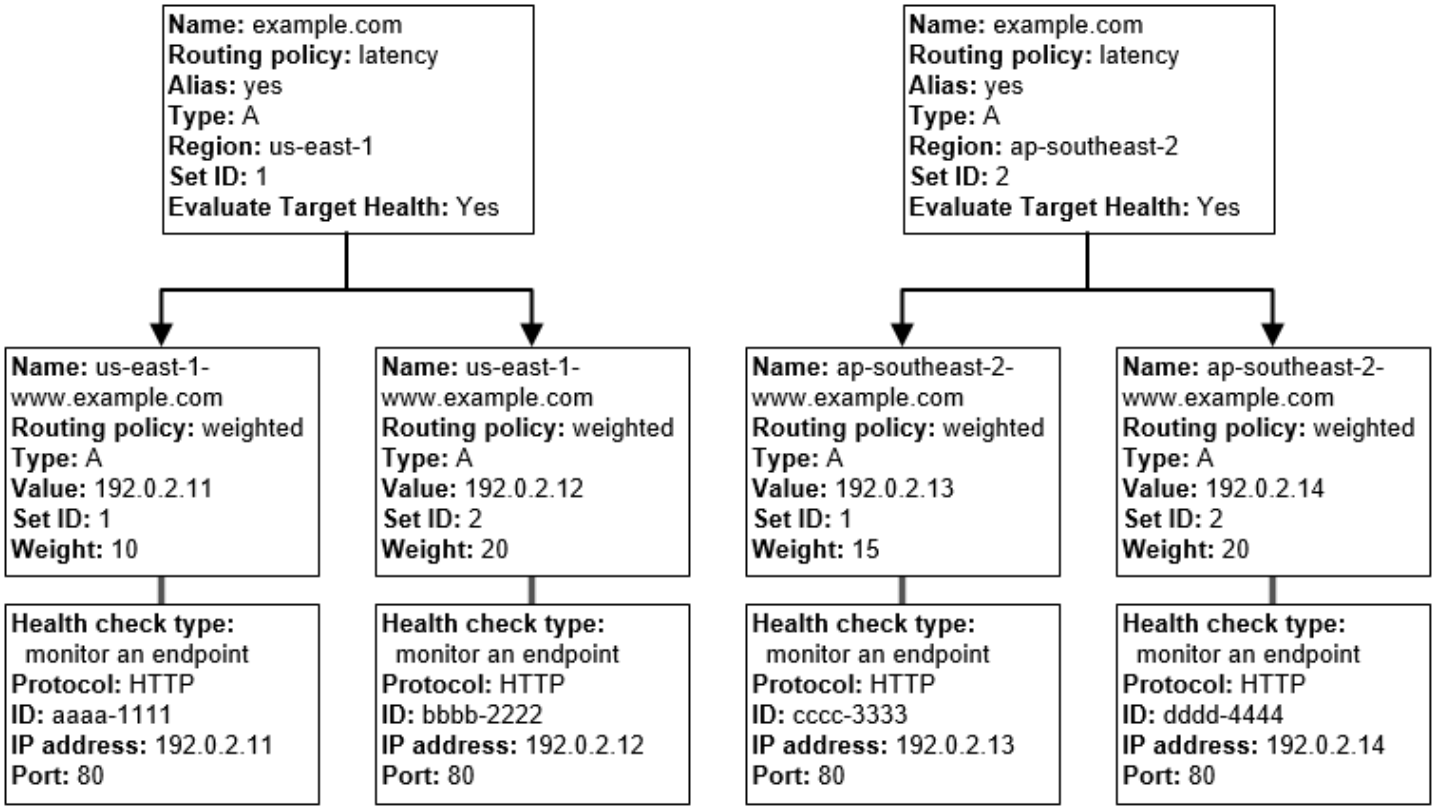
Se ometti un controllo dell'integrità da uno o più record di un gruppo di record, Route 53 non è in grado di determinare l'integrità della risorsa corrispondente. Route 53 tratta questi record come integri.



Funzionamento dei controlli dell'integrità in configurazioni complesse di Amazon Route 53

La verifica dell'integrità delle risorse in configurazioni complesse funziona come quella delle configurazioni semplici. Nelle configurazioni complesse, tuttavia, utilizzi una combinazione di record alias (ad esempio alias ponderati e di failover) e record non alias per creare un albero decisionale che offre un maggiore controllo sulle modalità con cui Route 53 risponde alle richieste.

Ad esempio, è possibile usare i record alias di latenza per selezionare una regione vicina a un utente e utilizzare record ponderati per due o più risorse all'interno di ciascuna regione per la protezione dall'errore di un singolo endpoint o di una zona di disponibilità. Il seguente diagramma mostra questa configurazione.



Ecco come sono configurati Amazon EC2 e Route 53. Cominciamo dalla parte inferiore dell'albero, perché è l'ordine in cui procederai alla creazione dei record:

- Sono disponibili due EC2 istanze in ciascuna delle due regioni, us-east-1 e ap-southeast-2. Vuoi che Route 53 indirizzi il traffico verso le tue EC2 istanze a seconda che siano funzionanti, quindi crei un controllo dello stato di salute per ogni istanza. Configura ogni controllo dell'integrità in modo da inviare le richieste di verifica dello stato all'istanza corrispondente presso l'indirizzo IP elastico per l'istanza.

  Route 53 è un servizio globale, perciò non è necessario specificare la regione in cui desideri creare i controlli dell'integrità.
- Poiché l'obiettivo è instradare il traffico verso le due istanze in ciascuna regione in base al tipo di istanza, crea un record ponderato per ogni istanza e assegna un peso a ciascuno. (Puoi modificare il peso in un secondo momento in modo da instradare più o meno traffico verso un'istanza). Associa a ciascuna istanza il controllo dell'integrità applicabile.

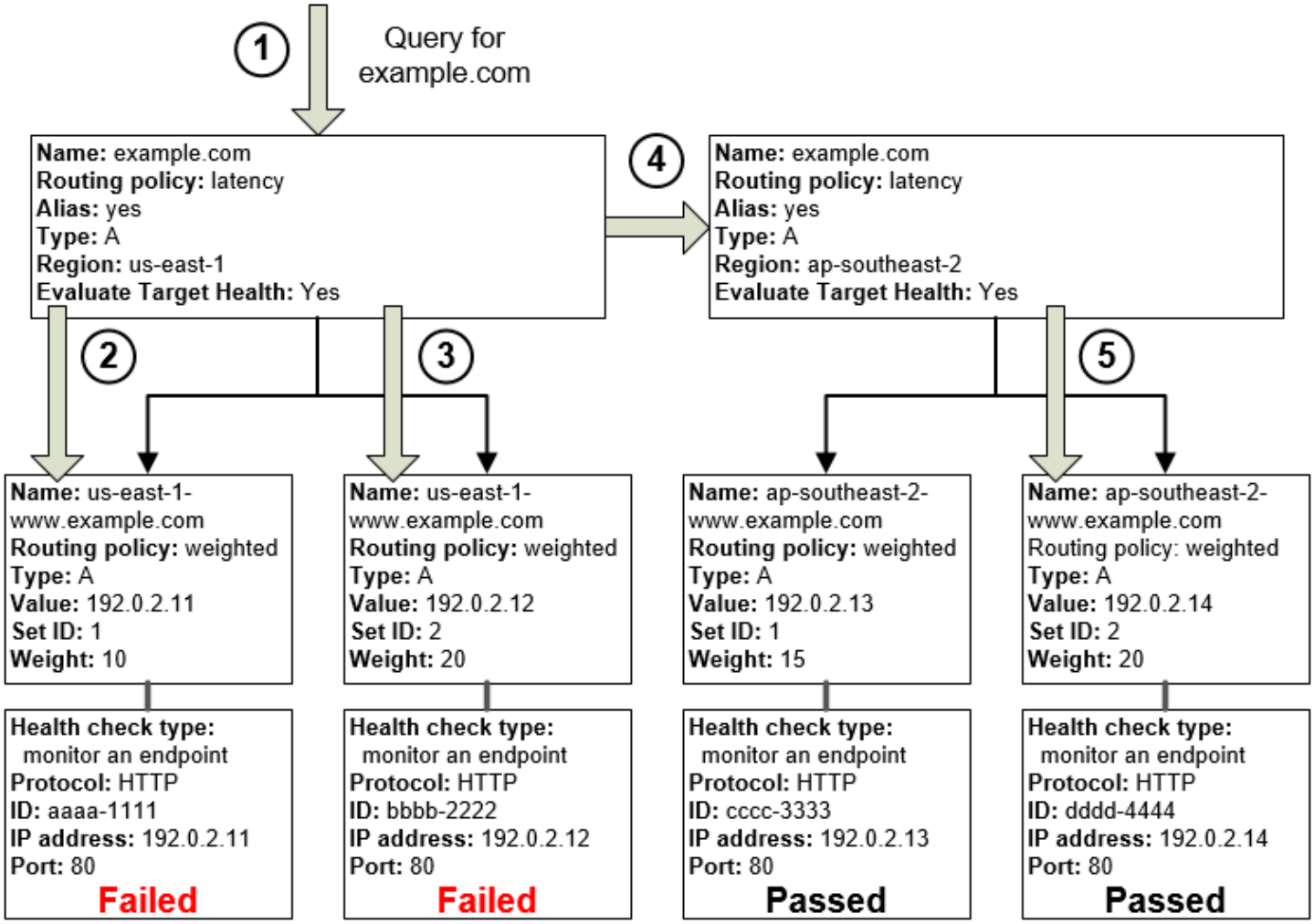
  Quando crei i record, utilizza nomi come us-east-1-www.esempio.com. e ap-southeast-2-www.esempio.com. Aspetta di arrivare in cima all'albero per assegnare ai record il nome che gli utenti utilizzeranno per accedere al tuo sito o alla tua applicazione Web, ad esempio esempio.com.

- Poiché il traffico deve essere instradato verso la regione che offre la latenza più bassa per i tuoi utenti, per i record nella parte superiore dell'albero scegli la policy di routing di latenza.

  Il traffico deve essere instradato verso i record in ciascuna regione, non direttamente verso le risorse in ciascuna regione (lo fanno già i record ponderati). Di conseguenza devi creare dei record alias di latenza.

  Quando crei i record alias, assegna loro il nome che vuoi che gli utenti utilizzino per accedere al tuo sito o alla tua applicazione Web (ad esempio esempio.com). I record alias instradano il traffico per esempio.com verso i record us-east-1-www.esempio.com e ap-southeast-2-www.esempio.com.

  Per entrambi i record alias di latenza devi impostare il valore di Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì). In questo modo, prima di provare a instradare il traffico, Route 53 determina se in quella regione vi sono risorse integre. In caso contrario, Route 53 seleziona una risorsa integra nell'altra regione.



Il diagramma precedente illustra la sequenza di eventi riportata di seguito:

1. Route 53 riceve una query per esempio.com. In base alla latenza per l'utente che effettua la richiesta, Route 53 seleziona il record alias di latenza per la regione us-east-1.
2. Route 53 seleziona un record ponderato in base al peso. Valuta integrità destinazione è Sì per il record alias di latenza, perciò Route 53 controlla l'integrità del record ponderato selezionato.
3. Il controllo dell'integrità non è riuscito, perciò Route 53 sceglie un altro record ponderato in base al peso e ne controlla l'integrità. Anche quel record non è integro.
4. Route 53 esce da questo ramo della struttura, cerca il record alias di latenza con la migliore latenza successiva e seleziona il record per ap-southeast-2.
5. Route 53 seleziona nuovamente un record in base al peso e quindi controlla l'integrità della risorsa selezionata. La risorsa è integra, pertanto Route 53 restituisce il valore applicabile in risposta alla query.

Argomenti

Cosa accade se si associa un controllo dell'integrità a un record alias?

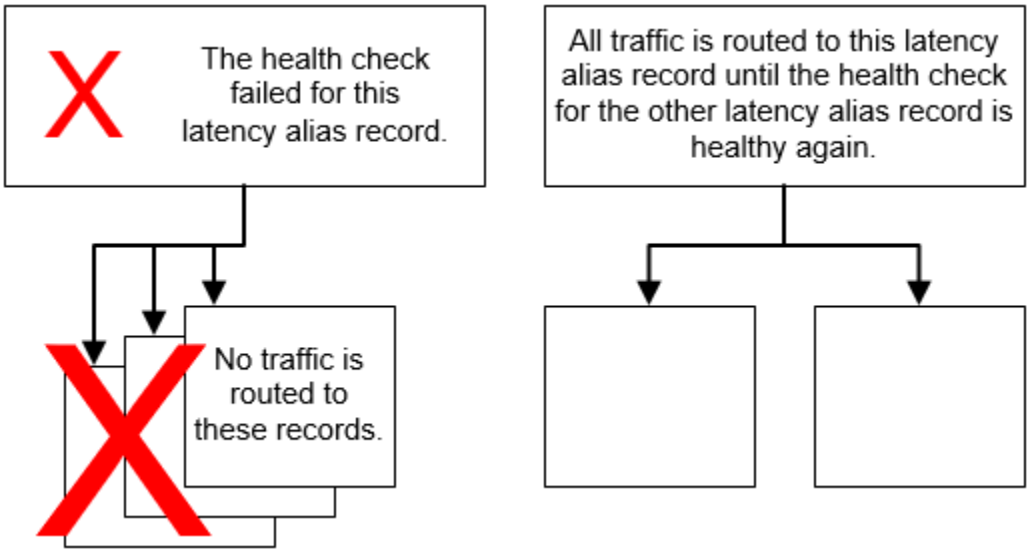
Puoi associare un controllo dell'integrità a un record alias anziché o in aggiunta all'impostazione del valore di Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì). Tuttavia, generalmente risulta più utile se Route 53 risponde alle query in base allo stato delle risorse sottostanti, ovvero i server HTTP, i server di database e altre risorse a cui i tuoi record alias fanno riferimento. Ad esempio, prendiamo come esempio la seguente configurazione:

- Assegni un controllo dell'integrità a un record alias di latenza per il quale la destinazione di alias è un gruppo di record ponderati.
- Imposta il valore di Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì) per il record alias di latenza.

In questa configurazione, prima che Route 53 restituisca il valore applicabile per un record ponderato entrambi i seguenti valori devono essere true:

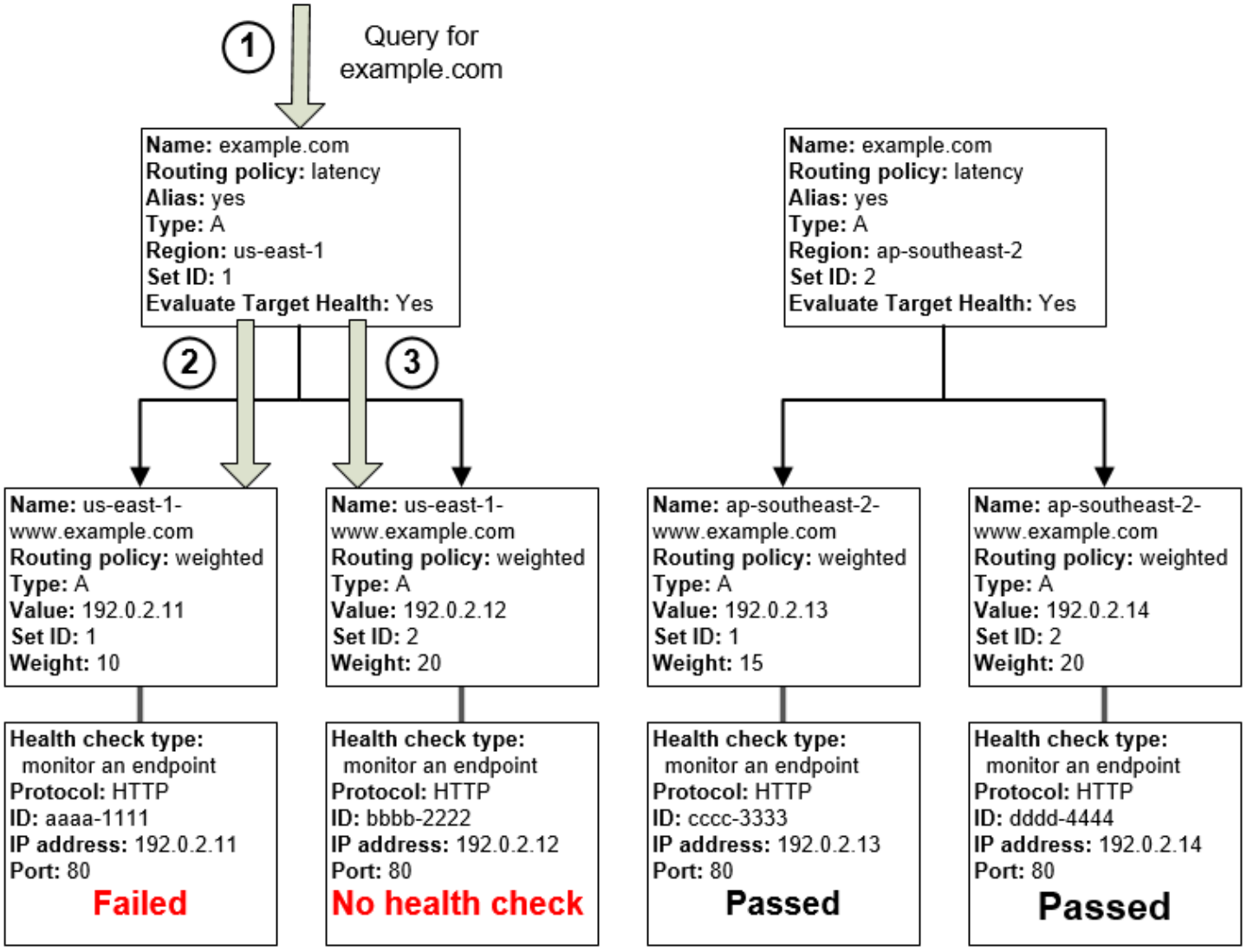
- Il controllo dell'integrità associato al record alias di latenza deve passare.
- Almeno un record ponderato deve essere considerato integro, perché è associato a un controllo dell'integrità che passa o perché non è associato a un controllo dell'integrità. In quest'ultimo caso, Route 53 considera sempre il record ponderato come integro.

Nell'illustrazione riportata di seguito, il controllo dell'integrità per i record alias di latenza in alto a sinistra ha avuto esito negativo. Di conseguenza, Route 53 smette di rispondere alle query utilizzando uno dei record ponderati a cui il record alias latenza fa riferimento anche qualora siano tutti integri. Route 53 comincia a considerare di nuovo i record ponderati solo quando il controllo dell'integrità per il record alias di latenza torna a essere integro. (Per le eccezioni, consulta Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità).



Cosa accade se si omettono i controlli dell'integrità?

In una configurazione complessa è importante associare controlli dell'integrità a tutti i record non alias. Nell'esempio seguente a uno dei record ponderati nella regione us-east-1 manca un controllo dell'integrità.



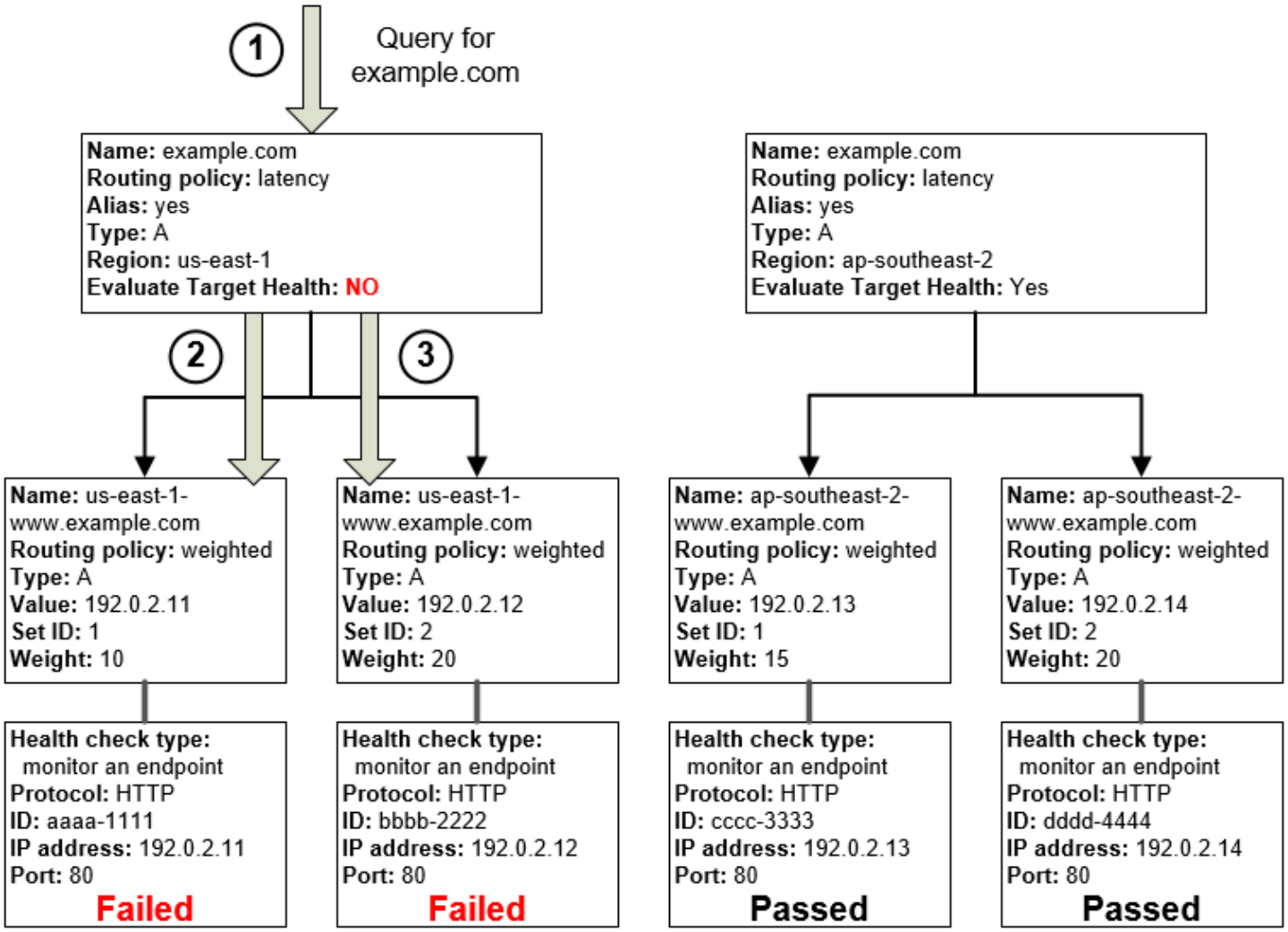
Ecco cosa succede quando si omette un controllo dell'integrità su un record alias in questa configurazione:

1. Route 53 riceve una query per esempio.com. In base alla latenza per l'utente che effettua la richiesta, Route 53 seleziona il record alias di latenza per la regione us-east-1.
2. Route 53 cerca la destinazione alias per il record alias di latenza e controlla lo stato dei controlli dell'integrità corrispondenti. Il controllo dell'integrità per un record ponderato non è riuscito, pertanto questo record non viene più preso in considerazione.
3. L'altro record ponderato nella destinazione alias per la regione us-east-1 non dispone di controllo dell'integrità. La risorsa corrispondente potrebbe essere o non essere integra, ma senza un controllo dell'integrità Route 53 non può saperlo. Route 53 presuppone che la risorsa sia integra e restituisce il valore applicabile in risposta alla query.

Cosa accade quando si la valutazione dello stato della destinazione su No?

In generale è consigliabile impostare Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì) per tutti i record alias presenti in un albero. Se imposti Valuta integrità destinazione su No, Route 53 continua a instradare il traffico verso i record ai quali un record alias fa riferimento anche se i controlli dell'integrità per i record hanno esito negativo.

Nel seguente esempio a tutti i record ponderati sono associati controlli dell'integrità, ma Evaluate Target Health (Valuta integrità destinazione) è impostato su No per il record alias di latenza relativo alla regione us-east-1:



Ecco cosa accade quando si imposta Evaluate Target Health (Valuta integrità destinazione) su No per un record alias in questa configurazione:

1. Route 53 riceve una query per esempio.com. In base alla latenza per l'utente che effettua la richiesta, Route 53 seleziona il record alias di latenza per la regione us-east-1.

2. Route 53 determina qual è la destinazione alias per il record alias di latenza e verifica i controlli dell'integrità corrispondenti. Entrambi stanno avendo esito negativo.
3. Poiché il valore di Valuta integrità destinazione è No per il record alias di latenza relativo alla regione us-east-1, Route 53 deve scegliere un record in questo ramo anziché uscire dallo stesso e cercare un record integro nella regione ap-southeast-2.

Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità

Se configuri il controllo dell'integrità per tutti i record in un gruppo di record aventi nome, tipo (ad esempio A o AAAA) e policy di routing (ad esempio ponderato o failover) identici, Route 53 risponde alle query DNS scegliendo un record integro e restituendo il valore applicabile da quel record.

Supponiamo ad esempio che crei tre record A ponderati e che assegni a tutti e tre un controllo dell'integrità. Se il controllo dell'integrità per uno dei record non è integro, Route 53 risponde alle query DNS con gli indirizzi IP in uno degli altri due record.

Ecco come Route 53 sceglie un record integro:

1. Route 53 sceglie dapprima un record in base alla policy di routing e ai valori che specifichi per ciascun record. Per i record ponderati, ad esempio, Route 53 sceglie un record in base al peso che specifichi per ciascun record.
2. Route 53 determina se il record è integro:
   - Record non alias con un controllo dell'integrità associato: se hai associato un controllo dell'integrità a un record non alias, Route 53 verifica lo stato corrente del controllo.

     Route 53 controlla periodicamente l'integrità dell'endpoint specificato in un controllo dell'integrità e non esegue il controllo quando arriva la query DNS.

     Associare i controlli dell'integrità a record alias è possibile, ma si consiglia di associarli solo ai record non alias. Per ulteriori informazioni, consulta Cosa accade se si associa un controllo dell'integrità a un record alias?.
   - Record di alias con valore Valuta integrità destinazione impostato su Sì: Route 53 controlla lo stato di integrità della risorsa alla quale il record alias fa riferimento, ad esempio un load balancer ELB o un altro record nella stessa zona ospitata.
3. Se il record è integro, Route 53 risponde alla query con il valore applicabile (ad esempio un indirizzo IP).

Se il record non è integro, Route 53 ne seleziona un altro utilizzando gli stessi criteri e ripete il processo finché non trova un record integro.

Per la scelta di un record, Route 53 adotta i seguenti criteri:

I record senza un controllo dell'integrità sono sempre integri

Se un record in un gruppo di record con nome e tipo identici non ha un controllo dell'integrità associato, Route 53 lo considera sempre integro e lo include sempre tra le possibili risposte a una query.

Se nessun record è integro, tutti i record sono integri

Se nessuno dei record in un gruppo di record è integro, Route 53 deve restituire qualcosa in risposta alle query DNS, ma non ha alcuna base per scegliere un record rispetto a un altro. In questo caso, Route 53 considera tutti i record del gruppo integri e ne seleziona uno in base alla policy di routing e ai valori specificati per ciascun record.

Record ponderati con un peso pari a 0

Se aggiungi controlli dell'integrità a tutti i record di un gruppo di record ponderati, ma ad alcuni record assegni un peso diverso da zero e ad altri un peso pari a zero, i controlli dell'integrità funzionano come se tutti i record avessero un peso diverso da zero, con le seguenti eccezioni:

- Route 53 inizialmente considera solo i record ponderati diversi da zero, se esistenti.
- Se tutti i record con un peso maggiore di 0 non sono integri, allora Route 53 considera i record con peso zero.

Poiché in alcune situazioni Route 53 prenderà in considerazione i record con peso zero, è importante assicurarsi che il target con peso zero abbia anche una risposta valida a una query DNS.

Per ulteriori informazioni sui record ponderati, consulta Controlli dell'integrità e routing ponderato.

Record alias

Puoi anche configurare il controllo dell'integrità per i record alias impostando Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì) per ciascun record alias. In questo modo Route 53 valuta l'integrità della risorsa verso cui il record instrada il traffico, ad esempio un load balancer ELB o un altro record nella stessa zona ospitata.

Supponiamo ad esempio che la destinazione alias per un record alias sia un gruppo di record ponderati aventi tutti un peso diverso da zero:

- Finché almeno uno dei record ponderati è integro, Route 53 considera il record alias integro.
- Se nessuno dei record ponderati è integro, Route 53 considera il record alias non integro.
- Route 53 smette di prendere in considerazione i record in quel ramo della struttura finché almeno un record ponderato non diventa nuovamente integro.

Per ulteriori informazioni, consulta Funzionamento dei controlli dell'integrità in configurazioni complesse di Amazon Route 53.

Record di failover

I record di failover in genere funzionano come gli altri tipi di routing. Crea i controlli dell'integrità e associali a record non alias e imposta Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì) per i record alias. Tieni presente quanto segue:

- Sia record principale sia quello secondario possono essere un record non alias o un record alias.
- Se associ i controlli dell'integrità sia al record di failover primario che a quello secondario, ecco come Route 53 risponde alle richieste:
  - Se Route 53 considera il record principale integro (se l'endpoint dei controlli dell'integrità è integro), in risposta a una query DNS Route 53 restituisce soltanto il record principale.
  - Se Route 53 considera il record principale non integro e il record secondario integro, restituisce invece il record secondario.
  - Se Route 53 considera sia il record principale sia il record secondario non integri, restituisce il record principale.
- Quando si configura il record secondario, l'aggiunta di un controllo dell'integrità è facoltativa. Se ometti il controllo dell'integrità per il record secondario e, se l'endpoint di controllo dell'integrità per il record primario è integro, Route 53 risponde sempre alle query DNS utilizzando il record secondario. Ciò è valido anche se il record secondario non è integro.

Per ulteriori informazioni, consulta i seguenti argomenti:

- Configurazione del failover attivo-passivo con una risorsa principale e una secondaria
- Configurazione del failover attivo-passivo con più risorse principali e secondarie

Failover attivo-attivo e attivo-passivo

Puoi utilizzare il controllo dell'integrità di Route 53 per impostare configurazioni di failover attivo-attivo e attivo-passivo. Configura il failover attivo-attivo utilizzando qualsiasi policy di routing (o combinazione di policy di routing) diversa dal failover e configura il failover attivo-passivo utilizzando la policy di routing di failover.

Argomenti

Failover attivo-attivo

Utilizza questa configurazione di failover quando vuoi che tutte le risorse siano disponibili per la maggior parte del tempo. Quando una risorsa non è più disponibile, Route 53 è in grado di rilevare che non è integra e smette di includerla quando risponde alle query.

Nel failover attivo-attivo tutti i record con nome, tipo (ad esempio A o AAAA) e policy di routing (ad esempio ponderato o latenza) identici sono attivi a meno che Route 53 non li consideri non integri. Route 53 può rispondere a una query DNS utilizzando qualsiasi record integro.

Failover attivo-passivo

Utilizza la configurazione di failover attivo-passivo quando vuoi che una risorsa o un gruppo di risorse principale sia disponibile per la maggior parte del tempo e che una risorsa secondaria o un gruppo di risorse secondario rimanga in standby nel caso in cui tutte le risorse principali non siano disponibili. Quando risponde alle query, Route 53 include solo le risorse primarie integre. Se tutte le risorse principali non sono integre, in risposta alle query DNS Route 53 comincia a includere solo le risorse secondarie integre.

Argomenti

Configurazione del failover attivo-passivo con una risorsa principale e una secondaria

Per creare una configurazione di failover attivo-passivo con un record principale e uno secondario, è sufficiente creare i record e specificare il Failover per la policy di routing. Quando la risorsa principale è integra, Route 53 risponde alle query DNS utilizzando il record primario. Quando la risorsa principale non è integra, Route 53 risponde alle query DNS utilizzando il record secondario.

Configurazione del failover attivo-passivo con più risorse principali e secondarie

Hai anche la possibilità di associare più risorse al record principale, al record secondario o a entrambi. In questa configurazione Route 53 considera il record di failover principale integro finché almeno una delle risorse associate è integra. Per ulteriori informazioni, consulta Come Amazon Route 53 sceglie i record quando viene configurato il controllo dell'integrità.

Per configurare il failover attivo-passivo con più risorse per il record principale o secondario, esegui le seguenti operazioni.

1. Crea un controllo dello stato di salute per ogni risorsa verso cui vuoi indirizzare il traffico, EC2 ad esempio un'istanza o un server web nel tuo data center.

   > **Note**
   >
   > Se stai indirizzando il traffico verso AWS risorse per le quali puoi creare record di alias, non creare controlli di integrità per tali risorse. Quando crei i record alias, invece, imposta il valore Evaluate Target Health (Valuta integrità destinazione) su Yes (Sì).

   Per ulteriori informazioni, consulta Creazione e aggiornamento di controlli dell'integrità.
2. Crea i record per le risorse principali e specifica i valori riportati di seguito:
   - Assegna nome, tipo e policy di routing identici a ogni record. Potresti ad esempio creare tre record A ponderati tutti con il nome failover-primary.esempio.com.
   - Se utilizzi AWS risorse per le quali puoi creare record di alias, specifica Sì per Evaluate Target Health.

     Se stai utilizzando risorse per le quali non è possibile creare record alias, associa a ogni record il controllo dell'integrità applicabile rifacendoti alla fase 1.

   Per ulteriori informazioni, consulta Creazione di record utilizzando la console Amazon Route 53.
3. Crea i record per le risorse secondarie e, se è il caso, specifica i valori riportati di seguito:

- Assegna nome, tipo e policy di routing identici a ogni record. Potresti ad esempio creare tre record A ponderati tutti con il nome failover-secondary.esempio.com.
- Se utilizzi AWS risorse per le quali puoi creare record di alias, specifica Sì per Evaluate Target Health.

  Se stai utilizzando risorse per le quali non è possibile creare record alias, associa a ogni record il controllo dell'integrità applicabile rifacendoti alla fase 1.

> **Note**
>
> Alcuni clienti utilizzano come risorsa principale un server Web e come risorsa secondaria un bucket Amazon S3 configurato come endpoint del sito Web. Il bucket S3 contiene un semplice messaggio "temporaneamente non disponibile". Se utilizzi tale configurazione, puoi ignorare questo passaggio e procedere a creare un record alias di failover per la risorsa secondaria nella fase 4.

4. Crea due record alias di failover, uno principale e uno secondario, e specifica i seguenti valori:

   Record principale

   - Nome: specifica il nome del dominio (esempio.com) o del sottodominio (www.esempio.com) verso il quale desideri che Route 53 instradi il traffico.
   - Alias: specifica Sì.
   - Destinazione alias: specifica il nome dei record creati nella fase 2.
   - Policy di routing: specifica Failover.
   - Tipo di record di failover: specifica Principale.
   - Valuta integrità destinazione: specifica Sì.
   - Associa a controllo dell'integrità: specifica No.

   Record secondario

   - Nome: specifica lo stesso nome specificato per il record principale.
   - Alias: specifica Sì.
   - Destinazione alias: se nella fase 3 hai creato i record per la tua risorsa secondaria, specifica qui il loro nome. Se stai utilizzando un bucket Amazon S3 per la risorsa secondaria, specifica il nome DNS dell'endpoint del sito Web.
   - Policy di routing: specifica Failover.
   - Tipo di record di failover: specifica Secondario.

- Valuta integrità destinazione: specifica Sì.
- Associa a controllo dell'integrità: specifica No.

Configurazione di un failover attivo-passivo con record ponderati

Hai anche la possibilità di utilizzare record ponderati per il failover attivo-passivo, con alcune avvertenze. Se specifichi un peso diverso da zero per alcuni record e un peso pari a zero per altri, Route 53 risponde alle query DNS utilizzando solo i record integri che hanno un peso diverso da zero. Se tutti i record con un peso maggiore di 0 non sono integri, Route 53 risponde alle query utilizzando i record con peso zero.

> **Note**
>
> Tutti i record con peso diverso da zero devono essere non integri prima che Route 53 cominci a rispondere alle query DNS utilizzando i record che hanno un peso pari a zero. Il tuo sito o la tua applicazione Web rischia di essere inaffidabile se l'ultima risorsa integra (ad esempio un server Web) non è in grado di gestire tutto il traffico quando le altre risorse non sono disponibili.

Configurazione del failover in una zona ospitata privata

Se stai creando record di failover in una zona ospitata privata, prendi nota di quanto segue:

- Gli strumenti di controllo dell'integrità di Route 53 sono all'esterno del VPC. Per controllare lo stato di un endpoint all'interno di un VPC mediante l'indirizzo IP, devi assegnare un indirizzo IP pubblico all'istanza nel VPC.
- Puoi creare una CloudWatch metrica, associare un allarme alla metrica e quindi creare un controllo dello stato basato sul flusso di dati relativo all'allarme. Ad esempio, potresti creare una CloudWatch metrica che controlli lo stato della EC2 `StatusCheckFailed` metrica, aggiungere un allarme alla metrica e quindi creare un controllo dello stato basato sul flusso di dati dell'allarme per controllare le istanze all'interno di un Virtual Private Cloud (VPC) che hanno solo indirizzi IP privati. Per informazioni sulla creazione di CloudWatch metriche e allarmi utilizzando la CloudWatch console, consulta la Amazon CloudWatch User Guide.

Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private e Monitoraggio dei controlli sanitari tramite CloudWatch.

Come Amazon Route 53 evita i problemi di failover

Gli algoritmi di failover implementati da Route 53 sono progettati non solo per instradare il traffico a endpoint integri, ma anche per evitare il peggioramento di scenari negativi a causa di controlli dell'integrità e applicazioni configurati in modo errato, sovraccarichi di endpoint ed errori di partizione.

Argomenti

Come Amazon Route 53 evita gli errori a cascata

In quanto prima difesa contro errori di cascading, ogni algoritmo di routing delle richieste (come ponderato e di failover) dispone di una modalità di ultima istanza. In questa modalità particolare, se nessun record è considerato integro, l'algoritmo di Route 53 torna a considerare tutti i record integri.

Ad esempio, se tutte le istanze di un'applicazione, su diversi host, respingono le richieste di controllo dell'integrità, i server DNS di Route 53 sceglieranno una risposta comunque e la restituiranno invece di non restituire alcuna risposta DNS o di restituire una risposta NXDOMAIN (dominio inesistente). Un'applicazione è in grado di rispondere agli utenti ma i controlli dell'integrità hanno ancora esito negativo, pertanto questo offre una certa protezione contro la configurazione errata.

Analogamente, se un'applicazione è sovraccaricata e uno dei tre endpoint non supera i controlli dell'integrità così da essere escluso dalle risposte DNS di Route 53, Route 53 distribuisce le risposte tra i due endpoint rimanenti. Se gli endpoint rimanenti non sono in grado di gestire il carico aggiuntivo e hanno esito negativo, Route 53 torna a distribuire le richieste a tutti e tre gli endpoint.

Come Amazon Route 53 gestisce le partizioni Internet

Anche se capita di rado, a volte vi sono partizioni Internet notevoli, per cui grandi regioni geografiche non riescono a comunicare via Internet. Durante queste partizioni, le posizioni Route 53 potrebbero giungere a conclusioni diverse sullo stato di salute di un endpoint e potrebbero differire dallo stato a cui sono state riportate. CloudWatch Gli addetti al controllo dello stato di salute della Route 53 in ogni AWS regione inviano costantemente gli stati dei controlli sanitari a tutte le sedi della Route 53. Durante le partizioni Internet, ogni posizione di Route 53 può avere accesso solo a un set parziale di questi stati, di solito dalle regioni più vicine.

Durante una partizione di Internet che interessa la connettività da e verso il Sud America, ad esempio, i server DNS di Route 53 nella posizione Sud America (San Paolo) potrebbero avere un

buon accesso agli endpoint del controllo dell'integrità nella regione AWS Sud America (San Paolo), ma uno scarso accesso agli endpoint situati altrove. Al contempo nella regione Stati Uniti orientali (Ohio) Route 53 potrebbe avere uno scarso accesso agli endpoint del controllo dell'integrità nella regione Sud America (San Paolo) e concludere che i record corrispondenti non sono integri.

Partizioni come queste possono provocare situazioni in cui le posizioni di Route 53 giungono a conclusioni diverse sullo stato di endpoint, in base alla loro visibilità locale di questi endpoint. Per questo motivo, ogni posizione di Route 53 considera un endpoint integro solo quando una porzione degli strumenti di controllo dell'integrità raggiungibili lo considera sano.

Denominazione e tagging di controlli dell'integrità

Puoi aggiungere tag a controlli dell'integrità di Amazon Route 53 che ti consentono di fornire a ogni controllo dell'integrità un nome più comprensibile rispetto all'ID del controllo dell'integrità. Si tratta degli stessi tag che AWS Billing and Cost Management consentono di organizzare la fattura. AWS Per ulteriori informazioni sull'utilizzo di tag per l'allocazione dei costi, consulta Utilizzo di tag per l'allocazione dei costi per report di fatturazione personalizzati nella Guida per l'utente di AWS Billing .

Ogni tag consiste di una chiave (il nome del tag) e di un valore, entrambi personalizzabili. Quando aggiungi i tag a un controllo dell'integrità, ti consigliamo di aggiungere un tag con i seguenti valori per la chiave e il valore:

- chiave: nome
- valore: il nome che desideri dare al controllo dell'integrità

Il valore del tag Nome viene visualizzato nell'elenco dei controlli dell'integrità nella console Route 53, che consente di distinguere tra loro velocemente i controlli dell'integrità. Per vedere altri tag per un controllo dell'integrità, scegli il controllo e quindi scegli la scheda Tags (Tag).

Per ulteriori informazioni sui tag, consulta i seguenti argomenti:

- Per aggiungere, modificare o eliminare il tag Nome quando si aggiunge o si modificano i controlli dell'integrità nella console Route 53, consulta Creazione e aggiornamento di controlli dell'integrità.
- Per una panoramica delle risorse di Route 53 per l'assegnazione di tag, consulta Assegnazione di tag alle risorse di Amazon Route 53.

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50 sulla nuova console e 10 sulla vecchia console.
- Lunghezza massima della chiave: 128 caratteri Unicode
- Lunghezza massima del valore: 256 caratteri Unicode
- Valori validi per Chiave e Valore: lettere maiuscole e minuscole nel set di caratteri UTF-8, numeri, spazi e i seguenti caratteri: _ . : / = + - e @.
- Chiavi e valori di tag fanno distinzione tra maiuscole e minuscole
- Non utilizzare il `aws:` prefisso né per le chiavi né per i valori; è AWS riservato all'uso

Aggiunta, modifica ed eliminazione di tag per controlli dell'integrità

Le procedure seguenti illustrano come usare i tag per i controlli dell'integrità nella console Route 53.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per aggiungere i tag ai controlli dello stato

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Seleziona l'ID collegato del controllo sanitario per il quale desideri aggiungere i tag.

4. Nella pagina inferiore, scegli la scheda Tag, quindi scegli Gestisci e quindi Aggiungi nuovi tag.
5. Inserisci un nome per il tag nel campo Chiave e inserisci un valore nel campo Valore.
6. Seleziona Salva.

Come modificare tag per i controlli dello stato

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Seleziona l'ID collegato di un controllo sanitario.
4. Nel riquadro inferiore, scegli la scheda Tag, quindi scegli Gestisci.
5. Ora puoi modificare e aggiungere altri tag.
6. Seleziona Salva.

Come eliminare tag per i controlli dello stato

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Seleziona l'ID collegato di un controllo sanitario.
4. Nel riquadro inferiore, scegli la scheda Tag, quindi scegli Gestisci.
5. Scegli Rimuovi accanto al tag che desideri eliminare.
6. Seleziona Salva.

Old console

Per aggiungere i tag ai controlli dello stato

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
3. Seleziona un controllo dell'integrità, oppure seleziona più controlli dell'integrità se desideri aggiungere lo stesso tag a più di un controllo dell'integrità.

4. Nel riquadro inferiore scegli la scheda Tags (Tag) e seleziona Add/Edit Tags (Aggiungi/Modifica tag).
5. Nella finestra di dialogo Add/Edit Tags (Aggiungi/Modifica tag), immetti un nome per il tag nel campo Key (Chiave) e un valore nel campo Value (Valore).
6. Scegli Apply changes (Applica modifiche).

Come modificare tag per i controlli dello stato

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
3. Selezionare un controllo dell'integrità.

   Se selezioni più controlli dell'integrità che condividono lo stesso tag, non puoi modificare il valore per tutti i tag contemporaneamente. Puoi però modificare il valore di un tag che viene visualizzato in più controlli dell'integrità se selezioni controlli dell'integrità che hanno il tag e almeno uno che non lo ha.

   Ad esempio, supponiamo di selezionare più controlli dell'integrità che hanno un tag Cost Center (Centro di costo) e uno che non ce l'ha. Puoi scegliere l'opzione che consente di aggiungere un tag e specificare Cost Center (Centro di costo) per la chiave e 777 per il valore. Per i controlli dell'integrità selezionati che dispongono già di un tag Centro di costo, Route 53 modifica il valore in 777. Per un controllo dell'integrità che non dispone di un tag Centro di costo, Route 53 ne aggiunge uno e imposta il valore su 777.
4. Nel riquadro inferiore scegli la scheda Tags (Tag) e seleziona Add/Edit Tags (Aggiungi/Modifica tag).
5. Nella finestra di dialogo Add/Edit Tags (Aggiungi/Modifica tag), modifica il valore.
6. Seleziona Salva.

Come eliminare tag per i controlli dello stato

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).

3. Seleziona un controllo dell'integrità, oppure seleziona più controlli dell'integrità se desideri eliminare lo stesso tag da più di un controllo dell'integrità.
4. Nel riquadro inferiore scegli la scheda Tags (Tag) e seleziona Add/Edit Tags (Aggiungi/Modifica tag).
5. Nella finestra di dialogo Aggiungi/Modifica tag, scegli il tag *X* accanto al tag che desideri eliminare.
6. Seleziona Salva.

Utilizzo dei controlli dell'integrità con versioni dell'API Amazon Route 53 precedenti al 2012-12-12

I controlli dell'integrità sono supportati a partire dalla versione del 2012-12-12 dell'API Amazon Route 53. Se una zona ospitata contiene record per i quali sono configurati controlli dell'integrità, ti consigliamo di usare solo l'API versione 12-12-2012 o successiva. Nota le seguenti limitazioni sull'utilizzo di controlli dell'integrità con le precedenti versioni dell'API.

- L'operazione `ChangeResourceRecordSets` non è in grado di creare o eliminare i record che includono gli elementi `EvaluateTargetHealth`, `Failovero` `HealthCheckId`.
- L'operazione `ListResourceRecordSets` è in grado di elencare record che includono questi elementi, ma gli elementi non sono inclusi nell'output. Al contrario, l'elemento `Value` della risposta contiene un messaggio indicante che il record include un attributo non supportato.

Monitoraggio dello stato del controllo dell'integrità e ricezione di notifiche

Puoi monitorare lo stato dei tuoi controlli dell'integrità dalla console Amazon Route 53. Puoi anche impostare CloudWatch allarmi e ricevere notifiche automatiche quando lo stato del tuo controllo sanitario cambia.

Argomenti

Visualizzazione dello stato del controllo dell'integrità e motivo degli errori del controllo dell'integrità

Nella console Route 53 puoi visualizzare lo stato (integro o non integro) dei controlli dell'integrità come riportato dagli strumenti di controllo dell'integrità di Route 53. Per tutti i controlli dell'integrità eccetto i controlli dell'integrità calcolati è anche possibile visualizzare i motivi per l'ultimo errore di controllo dell'integrità, ad esempio, se gli strumenti di controllo dell'integrità non sono stati in grado di stabilire una connessione con l'endpoint.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

New console

Per visualizzare lo stato e il motivo dell'ultimo errore di un controllo sanitario

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Per una panoramica dello stato di tutti i tuoi controlli dell'integrità, integro o non integro, visualizza la colonna Stato. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.
4. Per tutti i controlli dell'integrità eccetto i controlli dell'integrità calcolati, puoi visualizzare lo stato degli strumenti di controllo dell'integrità di Route 53 che non controllano l'integrità di un endpoint specificato.
5. Scegli l'ID collegato del controllo sanitario di cui desideri visualizzare i dettagli.
6. Nel riquadro inferiore, scegli la scheda Health checkers.

> **Note**
>
> Prima che lo stato del controllo dell'integrità e l'ultimo motivo di errore appaiano nella colonna Stato, i nuovi controlli dell'integrità devono propagarsi agli strumenti di controllo dell'integrità di Route 53. Fino al termine della propagazione, il messaggio nella colonna spiega che lo stato non è disponibile.

7. La tabella include i seguenti valori:

   IP dello strumento di controllo dell'integrità

   L'indirizzo IP dello strumento di controllo dell'integrità di Route 53 che ha eseguito il controllo dell'integrità.

   Ultima verifica

   La data e l'ora del controllo sanitario o la data e l'ora dell'ultimo fallimento.

   Stato

   Lo stato attuale del controllo sanitario o il motivo dell'ultimo fallimento del controllo sanitario.

Old console

Per visualizzare lo stato e il motivo dell'ultimo fallimento di un controllo sanitario

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
3. Per una panoramica dello stato di tutti i tuoi controlli dell'integrità, integro o non integro, visualizza la colonna Stato. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.
4. Per tutti i controlli dell'integrità eccetto i controlli dell'integrità calcolati, puoi visualizzare lo stato degli strumenti di controllo dell'integrità di Route 53 che non controllano l'integrità di un endpoint specificato. Selezionare il controllo dell'integrità.
5. Nel riquadro inferiore scegliere la scheda Health Checkers (Strumenti di controllo dell'integrità).

   > **Note**
   >
   > Prima che lo stato del controllo dell'integrità e l'ultimo motivo di errore appaiano nella colonna Stato, i nuovi controlli dell'integrità devono propagarsi agli strumenti di controllo dell'integrità di Route 53. Fino al termine della propagazione, il messaggio nella colonna spiega che lo stato non è disponibile.

6. Scegliere se si desidera visualizzare lo stato attuale del controllo dell'integrità o visualizzare la data e l'ora dell'ultimo errore e il motivo relativo. La tabella nella scheda Status (Stato) include i seguenti valori:

   IP dello strumento di controllo dell'integrità

   L'indirizzo IP dello strumento di controllo dell'integrità di Route 53 che ha eseguito il controllo dell'integrità.

   Ultima verifica

   La data e l'ora del controllo dell'integrità o la data e l'ora dell'ultimo errore, a seconda dell'opzione selezionata nella parte superiore della scheda Status (Stato).

Stato

Lo stato corrente del controllo dell'integrità o il motivo dell'errore dell'ultimo controllo dell'integrità, a seconda dell'opzione selezionata nella parte superiore della scheda Status (Stato).

Monitoraggio della latenza tra gli strumenti di controllo dell'integrità e l'endpoint

Quando crei un controllo di integrità, se scegli di monitorare lo stato di un endpoint (non lo stato di altri controlli di integrità) e scegli l'opzione Grafici di latenza, puoi visualizzare i seguenti valori sui CloudWatch grafici sulla console Route 53:

- Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per stabilire una connessione TCP con l'endpoint
- Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per ricevere il primo byte della risposta a una richiesta HTTP o HTTPS
- Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per completare l'handshake SSL/TLS

Note

Non è possibile abilitare il monitoraggio della latenza per controlli dell'integrità esistenti.

Important

I controlli di integrità vengono eseguiti in 16 zone di disponibilità ridondanti. Occasionalmente una zona di disponibilità può non essere disponibile a causa di distribuzioni, aggiornamenti, manutenzione e così via. Il sistema di controllo dell'integrità è progettato per tenere conto di questo senza alcun impatto sul cliente.

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per visualizzare la latenza tra i controllori dello stato di Route 53 e il tuo endpoint

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, scegli Health checks.
3. Seleziona l'ID collegato per il controllo sanitario di cui desideri visualizzare le metriche. È possibile visualizzare i dati di latenza per i controlli dell'integrità che monitorano lo stato di un endpoint e per cui l'opzione Latency graphs (Grafici di latenza) è abilitato.
4. Nel riquadro inferiore, scegli la scheda Metriche.
5. Scegliere l'intervallo di tempo e la regione geografica per la quale si desidera visualizzare grafici di latenza.

   I grafici visualizzano lo stato per l'intervallo di tempo specificato:

   Tempo di connessione TCP (solo HTTP e TCP)

   Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per stabilire una connessione TCP con l'endpoint.

   Tempo per il primo byte (solo HTTP e HTTPS)

   Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per ricevere il primo byte della risposta a una richiesta HTTP o HTTPS.

Tempo per completare l'handshake SSL (solo HTTPS)

Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per completare l'handshake SSL/TLS.

6. Per visualizzare un grafico più grande e specificare impostazioni diverse, scegli i tre punti in alto a destra del grafico. È possibile modificare le impostazioni seguenti:

   Statistic

   Modifica il calcolo che viene CloudWatch eseguito sui dati.

   Intervallo temporale

   Visualizza lo stato di un controllo dell'integrità per un periodo diverso, per esempio, di notte o l'ultima settimana.

   Periodo

   Modifica l'intervallo tra punti dati nel grafico.

   Tieni presente quanto segue:

   - Se hai appena creato un controllo dell'integrità, potrebbe essere necessario attendere alcuni minuti prima che vengano visualizzati i dati nel grafico e il parametro del controllo dell'integrità nell'elenco di parametri disponibili.
   - Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento ().
   - Se i controlli dell'integrità non hanno esito positivo per qualsiasi motivo, ad esempio un timeout di connessione, Route 53 non sarà in grado di misurare la latenza e i relativi dati non saranno riportati nel grafico per il periodo interessato.

Old console

Per visualizzare la latenza tra gli health checker di Route 53 e l'endpoint

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).

3. Selezionare le righe per i controlli dell'integrità applicabili. È possibile visualizzare i dati di latenza per i controlli dell'integrità che monitorano lo stato di un endpoint e per cui l'opzione Latency graphs (Grafici di latenza) è abilitato.
4. Nel riquadro inferiore scegliere la scheda Latency (Latenza).
5. Scegliere l'intervallo di tempo e la regione geografica per la quale si desidera visualizzare grafici di latenza.

   I grafici visualizzano lo stato per l'intervallo di tempo specificato:

   Tempo di connessione TCP (solo HTTP e TCP)

   Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per stabilire una connessione TCP con l'endpoint.

   Tempo per il primo byte (solo HTTP e HTTPS)

   Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per ricevere il primo byte della risposta a una richiesta HTTP o HTTPS.

   Tempo per completare l'handshake SSL (solo HTTPS)

   Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 nella regione geografica selezionata per completare l'handshake SSL/TLS.

   > **Note**
   >
   > Se si seleziona più di un controllo dell'integrità, il grafico visualizza una riga con codice colore separata per ogni controllo dell'integrità.

6. Per visualizzare un grafico di dimensioni maggiori e specificare impostazioni diverse, fare clic sul grafico. È possibile modificare le impostazioni seguenti:

   Statistic

   Modifica il calcolo che CloudWatch viene eseguito sui dati.

Intervallo temporale

Visualizza lo stato di un controllo dell'integrità per un periodo diverso, per esempio, di notte o l'ultima settimana.

Periodo

Modifica l'intervallo tra punti dati nel grafico.

Tieni presente quanto segue:

- Se hai appena creato un controllo dell'integrità, potrebbe essere necessario attendere alcuni minuti prima che vengano visualizzati i dati nel grafico e il parametro del controllo dell'integrità nell'elenco di parametri disponibili.
- Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento ().
- Se i controlli dell'integrità non hanno esito positivo per qualsiasi motivo, ad esempio un timeout di connessione, Route 53 non sarà in grado di misurare la latenza e i relativi dati non saranno riportati nel grafico per il periodo interessato.

Monitoraggio dei controlli sanitari tramite CloudWatch

I controlli di integrità di Route 53 si integrano con CloudWatch le metriche in modo da poter effettuare le seguenti operazioni:

- Verificare che un controllo dell'integrità sia configurato correttamente.
- Esaminare lo stato di un controllo dell'integrità in un periodo di tempo specificato.
- Configura CloudWatch per inviare un avviso Amazon SNS quando lo stato di un controllo sanitario non è integro. Si noti che potrebbero passare alcuni minuti tra il momento in cui un controllo dell'integrità ha esito negativo e l'orario in cui si riceve la notifica SNS associata.

Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Argomenti

- Visualizza lo stato del tuo controllo sanitario
- Visualizza gli allarmi relativi ai controlli sanitari
- Visualizza le metriche relative al controllo dello stato di salute sulla console CloudWatch
- Crea un allarme con una notifica SNS

Visualizza lo stato del tuo controllo sanitario

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per visualizzare lo stato di un controllo sanitario

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Health checks.
3. Scegli l'ID collegato del controllo sanitario di cui desideri visualizzare le metriche.
4. Nel riquadro inferiore, scegli la scheda Metriche.

   I due grafici visualizzano lo stato per l'ultima ora a intervalli di un minuto:

   Stato del controllo dell'integrità

   Il grafico mostra la valutazione di Route 53 dell'integrità dell'endpoint .1 significa integro e 0 significa non integro.

Strumenti di controllo dell'integrità che segnalano l'endpoint come integro (%)

Per tutti i controlli dell'integrità che monitorano soltanto un endpoint, il grafico mostra la percentuale di strumenti di controllo dell'integrità di Route 53 che considerano l'endpoint selezionato come integro.

Quando un controllo dell'integrità è stato disabilitato, questo parametro non è disponibile.

Numero di controlli dell'integrità figlio integri

Solo per i controlli dell'integrità calcolati, il grafico mostra il numero di controlli dell'integrità figlio integri.

5. Per visualizzare un grafico più grande e specificare impostazioni diverse, scegli i tre punti in alto a destra, quindi Ingrandisci. È possibile modificare le impostazioni seguenti:

   Statistic

   Modifica il calcolo che viene CloudWatch eseguito sui dati.

   Intervallo temporale

   Visualizza lo stato di un controllo dell'integrità per un periodo diverso, per esempio, di notte o l'ultima settimana.

   Periodo

   Modifica l'intervallo tra punti dati nel grafico.

   Tieni presente quanto segue:

   - Se hai appena creato un controllo dell'integrità, potrebbe essere necessario attendere alcuni minuti prima che vengano visualizzati i dati nel grafico e il parametro del controllo dell'integrità nell'elenco di parametri disponibili.
   - Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento
     ().

Old console

Per visualizzare lo stato di un controllo sanitario (nuova console)

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, seleziona Health Checks (Controlli dello stato).
3. Scegliere le righe per i controlli dell'integrità applicabili.
4. Nel riquadro inferiore scegliere la scheda Monitoring (Monitoraggio).

   I due grafici visualizzano lo stato per l'ultima ora a intervalli di un minuto:

   Stato del controllo dell'integrità

   Il grafico mostra la valutazione di Route 53 dell'integrità dell'endpoint .1 significa integro e 0 significa non integro.

   Strumenti di controllo dell'integrità che segnalano l'endpoint come integro (%)

   Per tutti i controlli dell'integrità che monitorano soltanto un endpoint, il grafico mostra la percentuale di strumenti di controllo dell'integrità di Route 53 che considerano l'endpoint selezionato come integro.

   Quando un controllo dell'integrità è stato disabilitato, questo parametro non è disponibile.

   Numero di controlli dell'integrità figlio integri

   Solo per i controlli dell'integrità calcolati, il grafico mostra il numero di controlli dell'integrità figlio integri.

   > **Note**
   >
   > Se è stato selezionato più di un controllo dell'integrità, il grafico visualizza una riga con codice colore separata per ogni controllo dell'integrità.

5. Per visualizzare un grafico di dimensioni maggiori e specificare impostazioni diverse, fare clic sul grafico. È possibile modificare le impostazioni seguenti:

   Statistic

   Modifica il calcolo che CloudWatch viene eseguito sui dati.

Intervallo temporale

Visualizza lo stato di un controllo dell'integrità per un periodo diverso, per esempio, di notte o l'ultima settimana.

Periodo

Modifica l'intervallo tra punti dati nel grafico.

Tieni presente quanto segue:

- Se hai appena creato un controllo dell'integrità, potrebbe essere necessario attendere alcuni minuti prima che vengano visualizzati i dati nel grafico e il parametro del controllo dell'integrità nell'elenco di parametri disponibili.
- Il grafico non si aggiorna automaticamente. Per aggiornare la visualizzazione, scegliere l'icona di aggiornamento ().

Visualizza gli allarmi relativi ai controlli sanitari

> **Note**
>
> Stiamo aggiornando la console per i controlli sanitari per Route 53. Durante il periodo di transizione, puoi continuare a utilizzare la vecchia console.

Seleziona la scheda per la console che stai utilizzando.

- Nuova console
- Vecchia console

New console

Per visualizzare lo stato CloudWatch degli allarmi e modificare gli allarmi per Amazon Route 53

1. Nel riquadro di navigazione della console Route 53, scegli Health checks.
2. Scegli l'ID collegato del controllo sanitario per il quale desideri visualizzare gli allarmi.

3. Nella pagina dei dettagli, nella parte inferiore della pagina, scegli la scheda Allarmi.

   L'elenco Allarmi contiene tutti gli allarmi Route 53 che hai creato per il controllo sanitario selezionato.

   La colonna State (Stato) mostra lo stato corrente di ciascun allarme:

   OK

   CloudWatch ha accumulato statistiche sufficienti dai controlli di integrità di Route 53 per determinare che l'endpoint non soddisfa la soglia di allarme.

   DATI INSUFFICIENTI

   CloudWatch non ha accumulato statistiche sufficienti per determinare se l'endpoint soddisfa la soglia di allarme. Questo è lo stato iniziale di un nuovo allarme. Lo stato di allarme cambia anche in DATI INSUFFICIENTI se le CloudWatch metriche non sono disponibili o se si elimina il controllo di integrità senza eliminare l'allarme associato.

   ALLARME

   CloudWatch ha accumulato statistiche sufficienti dai controlli sanitari di Route 53 per determinare che l'endpoint soddisfa la soglia di allarme e inviare una notifica all'indirizzo e-mail specificato.

4. Per visualizzare un allarme nella CloudWatch console, che fornisce informazioni più dettagliate sull'allarme (ad esempio, una cronologia degli aggiornamenti dell'allarme e delle modifiche di stato), scegli il nome collegato dell'allarme. Puoi anche modificare l'allarme sulla CloudWatch console.
5. Per creare un nuovo CloudWatch allarme sulla CloudWatch console, scegli Crea un CloudWatch allarme. Per ulteriori informazioni, consulta Trovare e creare allarmi consigliati nella Guida per l'CloudWatch utente.

Old console

Per visualizzare lo stato CloudWatch degli allarmi e modificare gli allarmi per Amazon Route 53

1. Nel pannello di navigazione della console Route 53, seleziona Controlli dell'integrità.
2. Scegliere la riga per qualsiasi controllo dell'integrità.

3. Nel riquadro dei dettagli (dopo x Health Checks Selected (Controlli dello stato selezionati)), scegliere la giusta icona dell'accento circonflesso ( ).

   L'elenco degli CloudWatch allarmi contiene tutti gli allarmi Route 53 che hai creato utilizzando l'account corrente. AWS

   La colonna State (Stato) mostra lo stato corrente di ciascun allarme:

   OK

   CloudWatch ha accumulato statistiche sufficienti dai controlli sanitari di Route 53 per determinare che l'endpoint non soddisfa la soglia di allarme.

   DATI INSUFFICIENTI

   CloudWatch non ha accumulato statistiche sufficienti per determinare se l'endpoint soddisfa la soglia di allarme. Questo è lo stato iniziale di un nuovo allarme. Lo stato di allarme cambia anche in DATI INSUFFICIENTI se le CloudWatch metriche non sono disponibili o se si elimina il controllo di integrità senza eliminare l'allarme associato.

   ALLARME

   CloudWatch ha accumulato statistiche sufficienti dai controlli sanitari di Route 53 per determinare che l'endpoint soddisfa la soglia di allarme e inviare una notifica all'indirizzo e-mail specificato.
4. Per visualizzare o modificare le impostazioni di un allarme, scegli il nome dell'allarme.
5. Per visualizzare un avviso nella CloudWatch console, che fornisce informazioni più dettagliate sull'allarme (ad esempio, una cronologia degli aggiornamenti dell'avviso e delle modifiche di stato), scegli Visualizza nella colonna Altre opzioni relativa all'allarme.
6. Per visualizzare tutti gli CloudWatch allarmi che hai creato utilizzando l' AWS account corrente, inclusi gli allarmi per altri AWS servizi, scegli Visualizza tutti gli CloudWatch allarmi.
7. Per visualizzare tutte le CloudWatch metriche disponibili, incluse le metriche che non sono attualmente utilizzate dall' AWS account corrente, scegli Visualizza tutte le metriche. CloudWatch

Visualizza le metriche relative al controllo dello stato di salute sulla console CloudWatch

Per visualizzare le metriche di Route 53 sulla console CloudWatch

1. Accedi a AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Cambia la regione in Stati Uniti orientali (Virginia settentrionale). I parametri di Route 53 non sono disponibili se si seleziona qualsiasi altra regione come regione corrente.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Nella scheda All metrics (Tutti i parametri) scegliere Route 53.
5. Scegliere Health Check Metrics (Parametri di controllo dell'integrità).
6. Puoi anche configurare la notifica SNS sulla CloudWatch console. Per ulteriori informazioni, consulta Creare allarmi consigliati nella Guida per l'CloudWatch utente.

Crea un allarme con una notifica SNS

> **Note**
>
> La procedura seguente si applica solo alla vecchia console. La nuova console ti indirizza alla CloudWatch console per creare allarmi. Per ulteriori informazioni, consulta Trovare e creare allarmi consigliati nella Guida per l'CloudWatch utente.

Per ricevere una notifica Amazon SNS quando lo stato di un controllo sanitario non è integro (vecchia console)

1. Nel riquadro di navigazione della console Route 53, seleziona Controlli dell'integrità.
2. Scegliere la riga per il controllo dell'integrità applicabile.
3. Nel riquadro inferiore scegliere la scheda Alarms (Allarmi).

   La tabella elenca gli allarmi che hai già creato per questo controllo dell'integrità.
4. Scegli Crea allarme.
5. Specifica i seguenti valori:

Nome allarme

Inserisci il nome che desideri che Route 53 visualizzi nella colonna Nome nella scheda Allarmi.

Descrizione dell'allarme

(Facoltativo) Immetti un nome e una descrizione per l'allarme. Questo valore viene visualizzato nella console. CloudWatch

Invia notifica

Scegli se desideri che Route 53 invii notifiche se lo stato di questo controllo dell'integrità attiva un allarme.

Destinazione notifica (solo quando "Send notification" (Invia notifica) è "Yes" (Sì))

Se desideri CloudWatch inviare una notifica a un argomento SNS esistente, scegli l'argomento dall'elenco.

Se desideri CloudWatch inviare una notifica ma non a un argomento SNS esistente, esegui una delle seguenti operazioni:

- Se desideri CloudWatch inviare una notifica via e-mail, scegli Nuovo argomento SNS e continua con questa procedura.
- Se desideri CloudWatch inviare una notifica con un altro metodo, apri una nuova scheda del browser, vai alla console Amazon SNS e crea il nuovo argomento. Torna quindi alla console Route 53, scegli il nome del nuovo argomento dall'elenco Destinazione notifica e continua con questa procedura.

Nome argomento (solo se decidi di creare un nuovo argomento Amazon SNS)

Immetti un nome per il nuovo argomento Amazon SNS.

Indirizzi e-mail destinatari (solo se decidi di creare un nuovo argomento Amazon SNS)

Immetti l'indirizzo e-mail a cui desideri che Route 53 invii una notifica SNS quando un controllo dell'integrità attiva un allarme.

Destinazione allarme

Scegli il valore che desideri che Route 53 valuti per questo controllo dell'integrità:

- Stato del controllo dell'integrità: gli strumenti di controllo dell'integrità di Route 53 segnalano che il controllo è integro o non integro

- Strumenti di controllo dell'integrità che segnalano l'endpoint come integro (%) (controlli dell'integrità che monitorano solo un endpoint): la percentuale di strumenti di controllo dell'integrità di Route 53 che segnalano lo stato del controllo dell'integrità come integro
- Numero di controlli dell'integrità figli integri (solo controlli dell'integrità calcolati): il numero di controlli dell'integrità figli in un controllo dell'integrità calcolato che segnalano che lo stato del controllo dell'integrità è integro
- Tempo di connessione TCP (solo controlli dell'integrità HTTP e TCP): il tempo in millisecondi impiegato dagli strumenti di controllo dell'integrità di Route 53 per stabilire una connessione TCP con l'endpoint
- Tempo per completare l'handshake SSL (solo controlli dell'integrità HTTPS): il tempo in millisecondi impiegato dagli strumenti di controllo dell'integrità di Route 53 per completare l'handshake SSL/TLS
- Tempo per il primo byte (solo controlli dell'integrità HTTP e HTTPS): il tempo in millisecondi impiegato dagli strumenti di controllo dell'integrità di Route 53 per ricevere il primo byte della risposta a una richiesta HTTP o HTTPS

Destinazione allarme

Per gli obiettivi degli allarmi basati sulla latenza (tempo di connessione TCP, tempo di completamento dell'handshake SSL, tempo di completamento del primo byte), scegli se calcolare la latenza per i controllori sanitari di Route 53 in una regione specifica o per tutte le regioni (globale). CloudWatch

Nota che se scegli una regione, Route 53 misura la latenza solo due volte al minuto e il numero di campioni sarà inferiore se si scelgono tutte le regioni. Di conseguenza, i valori ultraperiferici sono più probabili. Per evitare notifiche di allarme spurie, si consiglia di specificare un numero maggiore di periodi consecutivi in cui il controllo dello stato deve avere esito negativo prima dell'invio di una notifica da parte di CloudWatch .

Condizione di soddisfazione

Utilizza le seguenti impostazioni per determinare quando deve attivare un allarme. CloudWatch

Destinazione allarme	Condizione consigliata	Descrizione
Stato del controllo dell'integrità	Minimum (Minimo) < 1	Gli strumenti di controllo dell'integrità di Route 53 segnalano quando l'endpoint non è integro.
Strumenti di controllo dell'integrità che segnalano l'endpoint come integro (%)	Average (Media) < Percentuale desiderata	Controlli dell'integrità che monitorano solo un endpoint: Route 53 considera lo stato di un controllo dell'integrità come integro quando meno del 18% degli strumenti di controllo dell'integrità segnalano che lo stato sia integro. Non scegliere Conteggio di esempio per questo parametro perché la gamma di conteggi di esempio può variare man mano che Route 53 aggiunge più regioni di controllo dell'integrità. Average (Media) rappresenterà sempre accuratamente la percentuale di strumenti di controllo che segnalano lo stato di un controllo dell'integrità.
Numero di controlli dell'integrità figlio integri	Minimum (Minimo) < numero desiderato di controlli dell'integrità figlio integri	La statistica Minimum (Minimo) restituisce il valore più restrittivo e rappresenta lo scenario peggiore.
TCP connection time (Tempo di connessione TCP)	Average (Media) > tempo desiderato in millisecondi	Average (Media) è un valore più coerente rispetto alle altre statistiche.

Destinazione allarme	Condizione consigliata	Descrizione
Time to complete SSL handshake (Tempo per completare l'handshake SSL)	Average (Media) > tempo desiderato in millisecondi	Average (Media) è un valore più coerente rispetto alle altre statistiche.
Time to first byte (Tempo per il primo byte)	Average (Media) > tempo desiderato in millisecondi	Average (Media) è un valore più coerente rispetto alle altre statistiche.

Per periodi almeno ***x*** consecutivi di ***y*** minutes/hours/day

Specifica il numero di periodi di tempo consecutivi che il valore specificato deve soddisfare i criteri prima che Route 53 invii la notifica. Specificare quindi la durata del periodo di tempo.

6. Quando scegli Crea, Amazon SNS invia un'e-mail con informazioni sul nuovo argomento SNS.
7. Nell'e-mail, scegli Confirm subscription (Conferma abbonamento). È necessario confermare l'iscrizione per iniziare a ricevere CloudWatch le notifiche.

Utilizzo di DNS Firewall per filtrare il traffico DNS in uscita

Con il DNS Firewall per Route 53 Resolver è possibile filtrare e regolare il traffico DNS in uscita per il proprio cloud privato virtuale. A tale scopo, è possibile creare raccolte riutilizzabili di regole di filtro nei gruppi di regole di DNS Firewall, associare i gruppi di regole al VPC e quindi monitorare l'attività nei record e nei parametri di DNS Firewall. In base all'attività, è possibile regolare di conseguenza il comportamento di DNS Firewall.

DNS Firewall fornisce protezione per le richieste DNS in uscita provenienti da. VPCs Queste richieste vengono instradate tramite Resolver per la risoluzione dei nomi di dominio. Un uso principale delle protezioni DNS Firewall è quello di aiutare a prevenire l'esfiltrazione DNS dei dati. L'esfiltrazione DNS può verificarsi quando un malintenzionato compromette un'istanza dell'applicazione nel VPC e quindi utilizza la ricerca DNS per inviare dati dal VPC a un dominio che controlla. Con DNS Firewall, è possibile monitorare e controllare i domini su cui le applicazioni possono eseguire query. Puoi negare l'accesso ai domini che sai essere non validi e consentire il passaggio di tutte le altre query. In alternativa, è possibile rifiutare l'accesso a tutti i domini ad eccezione di quelli che consideri esplicitamente attendibili.

È possibile utilizzare DNS Firewall anche per bloccare le richieste di risoluzione alle risorse in zone ospitate private (condivise o locali), inclusi i nomi degli endpoint VPC. Può anche bloccare le richieste di nomi di EC2 istanze Amazon pubblici o privati.

DNS Firewall è una funzionalità di Route 53 Resolver e non richiede alcuna configurazione aggiuntiva del Resolver per l'utilizzo.

AWS Firewall Manager supporta DNS Firewall

Puoi utilizzare Firewall Manager per configurare e gestire centralmente le associazioni dei gruppi di regole del firewall DNS per VPCs tutti i tuoi account in AWS Organizations. Firewall Manager aggiunge automaticamente le associazioni VPCs che rientrano nell'ambito della politica del firewall DNS di Firewall Manager. Per ulteriori informazioni, consulta AWS Firewall Managerla AWS WAF AWS Firewall Manager, e la Guida per AWS Shield Advanced gli sviluppatori.

Come funziona DNS Firewall con AWS Network Firewall

Firewall DNS e Network Firewall offrono entrambi filtri dei nomi di dominio, ma per diversi tipi di traffico. Con DNS Firewall e Network Firewall insieme, è possibile configurare il filtro basato su dominio per il traffico a livello di applicazione su due percorsi di rete diversi.

- DNS Firewall fornisce il filtro per le query DNS in uscita che passano attraverso il Route 53 Resolver dalle applicazioni all'interno del tuo. VPCs È inoltre possibile configurare DNS Firewall per inviare risposte personalizzate per le query a nomi di dominio bloccati.
- Network Firewall fornisce filtri sia per il traffico a livello di rete che di applicazione, ma non dispone di visibilità sulle query eseguite da Route 53 Resolver.

Per ulteriori informazioni su Network Firewall, consulta la Guida per gli sviluppatori di Network Firewall.

Come funziona DNS Firewall per il risolutore Route 53

DNS Firewall per Route 53 Resolver consente di controllare l'accesso ai siti e bloccare le minacce a livello di DNS per le query DNS in uscita dal VPC tramite Route 53 Resolver. Con DNS Firewall, definisci le regole di filtraggio dei nomi di dominio in gruppi di regole che associ al tuo. VPCs È possibile specificare elenchi di nomi di dominio da consentire o bloccare oppure le regole Route 53 Resolver DNS Firewall Advanced che offrono protezione dal tunneling DNS e dalle minacce basate su Domain Generation Algorithm (DGA). Puoi personalizzare le risposte per le query DNS che blocchi. Per le regole che contengono un elenco di domini, puoi anche perfezionare la regola per consentire la trasmissione di determinati tipi di query, come MX-Records.

DNS Firewall filtra solo il nome di dominio. Non risolve tale nome in un indirizzo IP da bloccare. Inoltre, DNS Firewall filtra il traffico DNS, ma non filtra altri protocolli a livello di applicazione, come HTTPS, SSH, TLS, FTP e così via.

Componenti e impostazioni di DNS Firewall per Route 53 Resolver

Gestire DNS Firewall con i seguenti componenti e impostazioni centrali.

Gruppo di regole DNS Firewall

> Definisce una raccolta denominata e riutilizzabile di regole di DNS Firewall per filtrare le query DNS. Si compila il gruppo di regole con le regole di filtraggio, quindi si associa il gruppo di regole a una o più regole. VPCs Quando associ un gruppo di regole a un VPC, si abilita il filtro DNS Firewall per il VPC. Quindi, quando Resolver riceve una query DNS per un VPC che ha un gruppo di regole associato, Resolver passa la query a DNS Firewall per il filtro.

Se associ più gruppi di regole a un singolo VPC, è necessario indicare il relativo ordine di elaborazione tramite l'impostazione di priorità in ogni associazione. DNS Firewall elabora i gruppi di regole per un VPC dall'impostazione della priorità numerica più bassa a salire.

Per ulteriori informazioni, consulta Gruppi di regole e regole in DNS Firewall.

Regola DNS Firewall

Definisce una regola di filtro per le query DNS in un gruppo di regole di DNS Firewall Ogni regola specifica un elenco di domini o una protezione DNS Firewall e un'azione da intraprendere sulle query DNS i cui domini corrispondono alle specifiche di dominio indicate nella regola. È possibile consentire (solo regole con elenchi di domini), bloccare o inviare avvisi sulle query corrispondenti. Nelle regole con elenchi di domini è inoltre possibile specificare i tipi di query per i domini dell'elenco, ad esempio è possibile bloccare o consentire un tipo di query MX per uno o più domini specifici. Puoi inoltre definire risposte personalizzate per le query bloccate.

Per quanto riguarda le regole DNS Firewall, è possibile bloccare o inviare avvisi solo in caso di query corrispondenti.

Ogni regola di un gruppo di regole ha un'impostazione di priorità univoca all'interno del gruppo di regole. DNS Firewall elabora le regole in un gruppo di regole a partire dalla priorità più bassa a salire.

Le regole di DNS Firewall esistono solo nel contesto del gruppo di regole in cui sono definite. Non è possibile riutilizzare una regola o fare riferimento a essa indipendentemente dal relativo gruppo di regole.

Per ulteriori informazioni, consulta Gruppi di regole e regole in DNS Firewall.

Elenco dei domini

Definisce una raccolta denominata e riutilizzabile di specifiche di dominio da utilizzare nel filtro DNS. Ogni regola in un gruppo di regole richiede un singolo elenco di domini. È possibile scegliere di specificare i domini a cui si desidera consentire l'accesso, i domini a cui si desidera negare l'accesso o una combinazione di entrambi. Puoi creare elenchi di domini personalizzati e utilizzare elenchi di domini che AWS gestiscono per te.

Per ulteriori informazioni, consulta Elenchi di domini di DNS Firewall per Route 53 Resolver.

Impostazione di reindirizzamento del dominio (solo elenchi di domini)

L'impostazione di reindirizzamento del dominio consente di configurare una regola del firewall DNS per ispezionare tutti i domini della catena di reindirizzamento DNS (impostazione

predefinita), come CNAME, DNAME e così via, oppure solo il primo dominio e considerare attendibile il resto. Se scegli di controllare l'intera catena di reindirizzamento DNS, devi aggiungere i domini successivi a un elenco di domini impostato su ALLOW nella regola. Se scegli di ispezionare l'intera catena di reindirizzamento DNS, devi aggiungere i domini successivi a un elenco di domini e impostare l'azione che desideri venga intrapresa dalla regola, ovvero ALLOW, BLOCK o ALERT.

Per ulteriori informazioni, consulta Impostazioni delle regole in DNS Firewall.

Tipo di query (solo elenchi di domini)

L'impostazione del tipo di query consente di configurare una regola DNS Firewall per filtrare un particolare tipo di query DNS. Se non si seleziona un tipo di query, la regola viene applicata a tutti i tipi di query DNS. Ad esempio, potresti voler bloccare tutti i tipi di query per un determinato dominio, ma consentire i record MX.

Per ulteriori informazioni, consulta Impostazioni delle regole in DNS Firewall.

Protezione DNS Firewall Advanced

Rileva le query DNS sospette sulla base di firme di minacce note nelle query DNS. Ogni regola in un gruppo di regole richiede una singola impostazione di protezione DNS Firewall Advanced. Puoi scegliere la protezione tra:

- Algoritmi di generazione di domini () DGAs

  DGAs vengono utilizzati dagli aggressori per generare un gran numero di domini per lanciare attacchi di malware.

- tunneling DNS

  Il tunneling DNS viene utilizzato dagli aggressori per esfiltrare dati dal client utilizzando il tunnel DNS senza stabilire una connessione di rete con il client.

In una regola DNS Firewall Advanced puoi scegliere di bloccare o avvisare una query che corrisponde alla minaccia. Gli algoritmi di protezione dalle minacce sono gestiti e aggiornati da. AWS

Per ulteriori informazioni, consulta Route 53 Resolver DNS Firewall avanzato.

Soglia di confidenza (solo protezione DNS Firewall Advanced)

La soglia di confidenza per la protezione dalle minacce DNS. È necessario fornire questo valore quando si crea una regola DNS Firewall Advanced. I valori del livello di confidenza significano:

- Alto: rileva solo le minacce più comprovate con una bassa percentuale di falsi positivi.
- Medio: fornisce un equilibrio tra il rilevamento delle minacce e i falsi positivi.
- Basso: offre il più alto tasso di rilevamento delle minacce, ma aumenta anche i falsi positivi.

Per ulteriori informazioni, consulta Impostazioni delle regole in DNS Firewall.

Associazione tra un gruppo di regole DNS Firewall e un VPC

Definisce una protezione per un VPC utilizzando un gruppo di regole di DNS Firewall e abilita la configurazione del DNS Firewall di Resolver per il VPC.

Se associ più gruppi di regole a un singolo VPC, è necessario indicare il relativo ordine di elaborazione tramite l'impostazione di priorità in ogni associazione. DNS Firewall elabora i gruppi di regole per un VPC dall'impostazione della priorità numerica più bassa a salire.

Per ulteriori informazioni, consulta Abilitazione delle protezioni DNS Firewall per Route 53 Resolver per il VPC.

Configurazione di DNS Firewall di Resolver per un VPC

Specifica in che modo Resolver deve gestire le protezioni di DNS Firewall a livello di VPC. Questa configurazione è attiva ogni volta che al VPC è associato almeno un gruppo di regole DNS Firewall.

Questa configurazione specifica il modo in cui Route 53 Resolver gestisce le query quando DNS Firewall non riesce a filtrarle. Per impostazione predefinita, se Resolver non riceve una risposta da DNS Firewall per una query, non viene chiuso e blocca la query.

Per ulteriori informazioni, consulta Configurazione del VPC di DNS Firewall.

Monitoraggio delle azioni del firewall DNS

Puoi utilizzare Amazon CloudWatch per monitorare il numero di query DNS filtrate dai gruppi di regole del firewall DNS. CloudWatch raccoglie ed elabora dati grezzi in metriche leggibili e quasi in tempo reale.

Per ulteriori informazioni, consulta Monitoraggio dei gruppi di regole del firewall DNS di Route 53 Resolver con Amazon CloudWatch.

Puoi usare Amazon EventBridge, un servizio serverless che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, per creare applicazioni scalabili basate sugli eventi.

Per ulteriori informazioni, consulta Gestione degli eventi del firewall DNS di Route 53 Resolver utilizzando Amazon EventBridge.

Come DNS Firewall per Route 53 Resolver filtra le query DNS

Quando un gruppo di regole di DNS Firewall è associato a Route 53 Resolver del VPC, il firewall filtra il seguente traffico:

- Query DNS che provengono da quel VPC e passano attraverso il DNS VPC.
- Query DNS che passano attraverso gli endpoint di Resolver dalle risorse on-premise allo stesso VPC che ha il DNS Firewall associato al relativo resolver.

Quando DNS Firewall riceve una query DNS, filtra la query utilizzando i gruppi di regole, le regole e le altre impostazioni configurate e invia i risultati al Resolver:

- DNS Firewall valuta la query DNS utilizzando i gruppi di regole associati al VPC fino a quando non trova una corrispondenza o esaurisce tutti i gruppi di regole. DNS Firewall valuta i gruppi di regole in ordine della priorità impostata nell'associazione, a partire dall'impostazione numerica più bassa. Per ulteriori informazioni, consulta Gruppi di regole e regole in DNS Firewall e Abilitazione delle protezioni DNS Firewall per Route 53 Resolver per il VPC.
- All'interno di ogni gruppo di regole, DNS Firewall valuta la query DNS rispetto all'elenco di domini di ogni regola o alle protezioni DNS Firewall Advanced finché non trova una corrispondenza o esaurisce tutte le regole. DNS Firewall valuta le regole in ordine di priorità, a partire dall'impostazione numerica più bassa. Per ulteriori informazioni, consulta Gruppi di regole e regole in DNS Firewall.
- Quando DNS Firewall trova una corrispondenza con l'elenco di domini di una regola o anomalie identificate dalle protezioni delle regole DNS Firewall Advanced, interrompe la valutazione della query e risponde a Resolver con il risultato. Se l'operazione è `alert`, DNS Firewall invia anche un avviso ai log del Resolver configurati. Per ulteriori informazioni, consulta Operazioni delle regole in DNS Firewall, Elenchi di domini di DNS Firewall per Route 53 Resolver e Route 53 Resolver DNS Firewall avanzato.
- Se DNS Firewall valuta tutti i gruppi di regole senza trovare una corrispondenza, risponde alla query come al solito.

Il Resolver instrada la query in base alla risposta dal DNS Firewall. Nel caso improbabile che il DNS Firewall non riesca a rispondere, Resolver applica la modalità di errore del DNS Firewall configurato del VPC. Per ulteriori informazioni, consulta Configurazione del VPC di DNS Firewall.

Fasi avanzate per l'utilizzo di DNS Firewall per Route 53 Resolver

Per implementare il filtro di DNS Firewall per Route 53 Resolver in Amazon Virtual Private Cloud (VPC), completa le seguenti fasi avanzate.

- Definisci il tuo approccio di filtraggio, i tuoi elenchi di domini o le protezioni del firewall DNS: decidi come filtrare le query, identifica le specifiche di dominio di cui avrai bisogno e definisci la logica da utilizzare per valutare le query. Ad esempio, puoi autorizzare tutte le query ad eccezione di quelle riportate in un elenco di domini non corretti noti. Oppure puoi fare il contrario e bloccare tutti i domini tranne quelli di un elenco di domini approvati, in quello che è noto come un approccio walled garden. Puoi creare e gestire i tuoi elenchi di specifiche di dominio approvate o bloccate e puoi utilizzare elenchi di domini che gestiscono per te. AWS Per quanto riguarda le protezioni DNS Firewall, puoi filtrare le query bloccandole tutte, oppure puoi avvisare in caso di traffico di query sospetto verso domini che potrebbero contenere anomalie associate a minacce (DGA, tunneling DNS) per testare le impostazioni del firewall DNS. Per ulteriori informazioni, consulta Elenchi di domini di DNS Firewall per Route 53 Resolver e Route 53 Resolver DNS Firewall avanzato.
- Creare un gruppo di regole firewall: in DNS Firewall crea un gruppo di regole per filtrare le query DNS per il VPC. È necessario creare un gruppo di regole in ogni regione in cui desideri utilizzarlo. Potresti anche voler separare il tuo comportamento di filtraggio in più di un gruppo di regole per riutilizzarlo in più scenari di filtraggio diversi. VPCs Per informazioni sui gruppi di regole, consulta Gruppi di regole e regole in DNS Firewall.
- Aggiungere e configurare le regole: aggiungi una regola al gruppo di regole per ogni elenco di dominio e comportamento di filtro che desideri sia fornito dal gruppo di regole. Definisci le impostazioni di priorità per le regole in modo che vengano elaborate nell'ordine corretto all'interno del gruppo di regole, assegnando la priorità più bassa alla regola che desideri valutare per prima. Per ulteriori informazioni sulle regole, consulta Gruppi di regole e regole in DNS Firewall.
- Associare il gruppo di regole al VPC: per iniziare a utilizzare il gruppo di regole DNS Firewall, associalo al VPC. Se per il VPC utilizzi più gruppi di regole, imposta la priorità di ogni associazione in modo che i gruppi di regole vengano elaborati nell'ordine corretto, assegnando la priorità più bassa al gruppo di regole che desideri valutare per primo. Per ulteriori informazioni, consulta Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver.
- (Facoltativo) Modificare la configurazione del firewall per il VPC: se desideri che Route 53 Resolver blocchi le query quando DNS Firewall non riesce a inviare una risposta, modifica la configurazione DNS Firewall del VPC nel Resolver. Per ulteriori informazioni, consulta Configurazione del VPC di DNS Firewall.

Utilizzo dei gruppi di regole di DNS Firewall per Route 53 Resolver in più regioni

Route 53 Resolver DNS Firewall è un servizio regionale, quindi gli oggetti creati in una AWS regione sono disponibili solo in quella regione. Per utilizzare lo stesso gruppo di regole in più di una regione, è necessario creare il gruppo in ciascuna regione.

L' AWS account che ha creato un gruppo di regole può condividerlo con altri account. AWS Per ulteriori informazioni, consulta Condivisione dei gruppi di regole del firewall DNS di Route 53 Resolver tra account AWS.

Disponibilità regionale per Route 53 Resolver DNS Firewall

Il firewall DNS è disponibile nelle seguenti versioni: Regioni AWS

- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacific (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Malesia)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Mumbai)
- Regione Asia Pacifico (Osaka-Locale)
- Asia Pacific (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Regione Canada (Centrale)
- Canada occidentale (Calgary)
- Regione Europa (Francoforte)
- Regione Europa (Irlanda)
- Regione Europa (Londra)

- Europa (Milano)
- Regione Europa (Parigi)
- Europa (Spagna)
- Europa (Stoccolma)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)
- US West (Oregon)
- Cina (Pechino)
- Cina (Ningxia)
- AWS GovCloud (US)

Introduzione a DNS Firewall per Route 53 Resolver

La console DNS Firewall include una procedura guidata che ti assiste nelle seguenti fasi per iniziare a utilizzare DNS Firewall:

- Crea gruppi di regole per ogni set di regole che desideri utilizzare.
- Per ogni regola, compila l'elenco di domini che desideri ispezionare. È possibile creare elenchi di domini personalizzati e utilizzare elenchi di domini AWS gestiti.
- Associa i tuoi gruppi di regole al VPCs luogo in cui desideri utilizzarli.

Esempio di walled garden di DNS Firewall per Route 53 Resolver

In questo tutorial verrà creato un gruppo di regole che blocca tutti i domini tranne un gruppo selezionato di domini considerati attendibili. Questo approccio è tipico di una piattaforma chiusa, o walled garden.

Come configurare un gruppo di regole DNS Firewall tramite la procedura guidata della console

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 3.

   - O -

   Accedi a AWS Management Console e apri il

   la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/
2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Nella pagina Gruppi di regole, scegli Aggiungi gruppo di regole.
5. Per il nome per il gruppo specifica **`WalledGardenExample`**.

   Nella sezione Tag, puoi facoltativamente inserire una coppia chiave-valore per un tag. I tag facilitano l'organizzazione e la gestione delle risorse AWS . Per ulteriori informazioni, consulta Assegnazione di tag alle risorse di Amazon Route 53.
6. Scegli Aggiungi gruppo di regole.
7. Nella pagina dei WalledGardenExampledettagli, scegli la scheda Regole, quindi Aggiungi regola.
8. Nel riquadro Dettagli regola, specifica il nome della regola **`BlockAll`**.
9. Nel riquadro Elenco dei domini, seleziona Aggiungi il mio elenco di domini.
10. In Scegli o crea un nuovo elenco di domini seleziona Crea un nuovo elenco di domini.
11. Inserisci un nome di elenco di domini**`AllDomains`**, quindi nella casella di testo Inserisci un dominio per riga, inserisci un asterisco:**`*`**.
12. Per l'impostazione del reindirizzamento del dominio, accetta l'impostazione predefinita e lascia vuoto il campo Tipo di interrogazione, facoltativo.
13. Per l'azione, seleziona BLOCCA e quindi lascia la risposta da inviare con l'impostazione predefinita di NODATA.
14. Scegli Aggiungi regola. La tua regola BlockAllviene visualizzata nella scheda Regole della WalledGardenExamplepagina.
15. Nella WalledGardenExamplepagina, scegli Aggiungi regola per aggiungere una seconda regola al tuo gruppo di regole.

16. Nel riquadro dei dettagli della regola, inserisci il nome della regola**`AllowSelectDomains`**.
17. Nel riquadro Elenco dei domini, seleziona Aggiungi il mio elenco di domini.
18. In Scegli o crea un nuovo elenco di domini seleziona Crea un nuovo elenco di domini.
19. Specifica un nome per l'elenco di domini **`ExampleDomains`**.
20. Nella casella di testo Inserisci un dominio per riga, nella prima riga, inserisci **`example.com`** e nella seconda riga, inserisci**`example.org`**.

    > **Note**
    >
    > Se desideri che la regola venga applicata anche ai sottodomini, dovrai aggiungere quei domini all'elenco. Ad esempio, per aggiungere tutti i sottodomini di esempio.com, aggiungi **`*.example.com`** all'elenco.

21. Per l'impostazione di reindirizzamento del dominio, accettate l'impostazione predefinita e lasciate vuoto il campo Tipo di interrogazione (facoltativo).
22. Per l'azione, seleziona CONSENTI.
23. Scegli Aggiungi regola. Le regole sono entrambe visualizzate nella scheda Regole della WalledGardenExamplepagina.
24. Nella scheda Regole della WalledGardenExamplepagina, puoi modificare l'ordine di valutazione delle regole nel tuo gruppo di regole selezionando il numero elencato nella colonna Priorità e digitando un nuovo numero. DNS Firewall valuta le regole a partire dall'impostazione di priorità più bassa, quindi la regola con la priorità più bassa è la prima a essere valutata. Per questo esempio, vogliamo innanzitutto che DNS Firewall identifichi e consenta le query DNS per l'elenco di selezione dei domini e quindi blocchi eventuali query rimanenti.

    Modifica la priorità della regola in modo che AllowSelectDomainsabbia una priorità più bassa.

A questo punto hai un gruppo di regole che consente solo query di dominio specifiche. Per iniziare a utilizzarla, è necessario associarla al VPCs punto in cui si desidera utilizzare il comportamento di filtraggio. Per ulteriori informazioni, consulta Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver.

Esempio di elenco di blocco di DNS Firewall per Route 53 Resolver

In questo tutorial viene creato un gruppo di regole che blocca i domini che sai essere dannosi. Aggiungerai anche un tipo di query DNS consentito per i domini nell'elenco bloccato. Il gruppo di regole consente tutte le altre richieste DNS in uscita tramite Route 53 Resolver.

Come configurare un elenco di blocco di DNS Firewall tramite la procedura guidata della console

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 3.

   - O -

   Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Nella pagina Gruppi di regole, scegli Aggiungi gruppo di regole.
5. Per il nome per il gruppo specifica **`BlockListExample`**.

   Nella sezione Tag, puoi facoltativamente inserire una coppia chiave-valore per un tag. I tag facilitano l'organizzazione e la gestione delle risorse AWS . Per ulteriori informazioni, consulta Assegnazione di tag alle risorse di Amazon Route 53.
6. Nella pagina dei BlockListExampledettagli, scegli la scheda Regole, quindi Aggiungi regola.
7. Nel riquadro Dettagli regola, specifica il nome della regola **`BlockList`**.
8. Nel riquadro Elenco dei domini, seleziona Aggiungi il mio elenco di domini.
9. In Scegli o crea un nuovo elenco di domini seleziona Crea un nuovo elenco di domini.
10. Specifica il nome dell'elenco di domini **`MaliciousDomains`**, quindi casella di testo specifica i domini che desideri bloccare. Ad esempio **`example.org`**. Specifica un dominio per riga.

> **Note**
>
> Se desideri che la regola venga applicata anche ai sottodomini, dovrai aggiungere all'elenco anche quei domini. Ad esempio, per aggiungere tutti i sottodomini di esempio.org, aggiungi **`*.example.org`** all'elenco.

11. Per l'impostazione del reindirizzamento del dominio, accetta l'impostazione predefinita e lascia vuoto il campo Tipo di interrogazione (facoltativo).
12. Per l'operazione, seleziona BLOCK quindi lascia il valore di default NODATA per la risposta da inviare.
13. Scegli Aggiungi regola. La regola viene visualizzata nella scheda Regole della BlockListExamplepagina
14. nella scheda Regole della BlockedListExamplepagina, puoi modificare l'ordine di valutazione delle regole nel tuo gruppo di regole selezionando il numero elencato nella colonna Priorità e digitando un nuovo numero. DNS Firewall valuta le regole a partire dall'impostazione di priorità più bassa, quindi la regola con la priorità più bassa è la prima a essere valutata.

    Seleziona e regola la priorità della regola in modo che BlockListvenga valutata prima o dopo qualsiasi altra regola che potresti avere. La maggior parte delle volte, i domini dannosi noti dovrebbero essere bloccati per primi. In altre parole, le regole ad essi associate dovrebbero avere la priorità più bassa.
15. Per aggiungere una regola che consenta i record MX per i BlockList domini, nella pagina dei BlockedListExampledettagli della scheda Regole, scegli Aggiungi regola.
16. Nel riquadro Dettagli regola, specifica il nome della regola **`BlockList-allowMX`**.
17. Nel riquadro Elenco dei domini, seleziona Aggiungi il mio elenco di domini.
18. In Scegli o crea un nuovo elenco di domini, seleziona**`MaliciousDomains`**.
19. Per l'impostazione di reindirizzamento del dominio, accetta l'impostazione predefinita.
20. Nell'elenco dei tipi di query DNS, selezionare MX: specifica i server di posta.
21. Per l'operazione, seleziona ALLOW.
22. Scegli Aggiungi regola.
23. nella scheda Regole della BlockedListExamplepagina, puoi modificare l'ordine di valutazione delle regole nel tuo gruppo di regole selezionando il numero elencato nella colonna Priorità e digitando un nuovo numero. DNS Firewall valuta le regole a partire dall'impostazione di priorità più bassa, quindi la regola con la priorità più bassa è la prima a essere valutata.

Seleziona e regola la priorità della regola in modo che BlockList-AllowMX venga valutato prima o dopo qualsiasi altra regola che potresti avere. Poiché desideri consentire le interrogazioni MX, assicurati che la regola BlockList-AllowMX abbia una priorità inferiore a. BlockList

Ora disponi di un gruppo di regole che blocca specifiche query di dominio dannose, ma consente un tipo di query DNS specifico. Per iniziare a utilizzarlo, lo associ al VPCs punto in cui desideri utilizzare il comportamento di filtraggio. Per ulteriori informazioni, consulta Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver.

Gruppi di regole e regole in DNS Firewall

Questa sezione descrive le impostazioni che è possibile configurare per i gruppi di regole e le regole del firewall DNS, per definire il comportamento del firewall DNS per l'utente. VPCs Viene inoltre descritto come gestire le impostazioni per le regole e i gruppi di regole.

Quando i gruppi di regole sono configurati nel modo desiderato, è possibile utilizzarli direttamente e condividerli e gestirli tra gli account e nell'intera organizzazione in AWS Organizations.

- È possibile associare un gruppo di regole a più VPCs regole per garantire un comportamento coerente in tutta l'organizzazione. Per informazioni, consultare Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver.
- È possibile condividere gruppi di regole tra più account per una gestione coerente delle query DNS all'interno dell'organizzazione. Per informazioni, consultare Condivisione dei gruppi di regole del firewall DNS di Route 53 Resolver tra account AWS.
- È possibile utilizzare i gruppi di regole in tutta l'organizzazione AWS Organizations gestendoli nelle AWS Firewall Manager politiche. Per informazioni su Firewall Manager, consulta AWS Firewall Managerla Guida per AWS WAF gli AWS Shield Advanced sviluppatori e AWS Firewall Manager la Guida per gli sviluppatori.

Impostazioni del gruppo di regole in DNS Firewall

Quando crei o modifichi un gruppo di regole di DNS Firewall, devi specificare i seguenti valori:

Nome

Un nome univoco che ti consenta di trovare facilmente un gruppo di regole nel pannello di controllo.

(Facoltativo) Descrizione

Una breve descrizione che fornisce più contesto per il gruppo di regole.

Regione

La AWS regione scelta al momento della creazione del gruppo di regole. Un gruppo di regole creato in una regione è disponibile solo in quella regione. Per utilizzare lo stesso gruppo di regole in più di una regione, è necessario creare il gruppo in ciascuna regione.

Regolamento

Il comportamento di filtraggio delle regole è contenuto nelle relative regole. Per ulteriori informazioni, consulta la sezione seguente.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS fattura. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Impostazioni delle regole in DNS Firewall

Quando crei o modifichi una regola in un gruppo di regole di DNS Firewall, devi specificare i seguenti valori:

Nome

Un identificatore univoco per la regola nel gruppo di regole.

(Facoltativo) Descrizione

Una breve descrizione che fornisce ulteriori informazioni sulla regola.

Elenco dei domini

L'elenco dei domini controllati dalla regola. È possibile creare elenchi di dominio personalizzati o sottoscrivere un elenco di domini gestiti automaticamente da AWS . Per ulteriori informazioni, consulta Elenchi di domini di DNS Firewall per Route 53 Resolver.

Una regola può contenere un elenco di domini o una protezione DNS Firewall Advanced, ma non entrambe.

Impostazione di reindirizzamento del dominio (solo elenchi di domini)

Puoi scegliere che la regola DNS Firewall ispezioni solo il primo dominio o tutti (impostazione predefinita) i domini della catena di reindirizzamento DNS, come CNAME, DNAME, ecc. Se scegli di ispezionare tutti i domini, devi aggiungere i domini successivi nella catena di reindirizzamento DNS all'elenco dei domini e impostare l'azione che desideri venga intrapresa dalla regola, ovvero ALLOW, BLOCK o ALERT. Per ulteriori informazioni, consulta Componenti e impostazioni di DNS Firewall per Route 53 Resolver.

Tipo di query (solo elenchi di domini)

L'elenco dei tipi di query DNS esaminati dalla regola. I valori validi sono i seguenti:

- R: Restituisce un IPv4 indirizzo.
- AAAA: restituisce un indirizzo Ipv6.
- CAA: limita chi può creare certificazioni CAs SSL/TLS per il dominio.
- CNAME: restituisce un altro nome di dominio.
- DS: record che identifica la chiave di firma DNSSEC di una zona delegata.
- MX: specifica i server di posta.
- NAPTR: Regular-expression-based riscrittura dei nomi di dominio.
- NS: server di nomi autorevoli.
- PTR: associa un indirizzo IP a un nome di dominio.
- SOA: inizio del record di autorità per la zona.
- SPF: elenca i server autorizzati a inviare e-mail da un dominio.
- SRV: valori specifici dell'applicazione che identificano i server.
- TXT: verifica i mittenti di posta elettronica e i valori specifici dell'applicazione.
- Un tipo di query definito utilizzando l'ID del tipo DNS, ad esempio 28 per AAAA. I valori devono essere definiti come TYPE*NUMBER*, dove ad esempio *NUMBER* può essere 1-65334. TYPE28 Per ulteriori informazioni, vedere Elenco dei tipi di record DNS.

  È possibile creare un tipo di query per regola.

> **Note**
>
> Se si imposta una regola BLOCK del firewall con l'azione NXDOMAIN sul tipo di query uguale a AAAA, questa azione non verrà applicata agli IPv6 indirizzi sintetici generati quando è abilitata. DNS64

Protezione DNS Firewall Advanced

Rileva le query DNS sospette sulla base di firme di minacce note nelle query DNS. Puoi scegliere la protezione tra:

- Algoritmi di generazione di domini () DGAs

  DGAs vengono utilizzati dagli aggressori per generare un gran numero di domini per lanciare attacchi di malware.

- tunneling DNS

  Il tunneling DNS viene utilizzato dagli aggressori per esfiltrare dati dal client utilizzando il tunnel DNS senza stabilire una connessione di rete con il client.

In una regola DNS Firewall Advanced puoi scegliere di bloccare o avvisare una query che corrisponde alla minaccia.

Per ulteriori informazioni, consulta Route 53 Resolver DNS Firewall avanzato.

Una regola può contenere una protezione DNS Firewall Advanced o un elenco di domini, ma non entrambi.

Soglia di confidenza (solo DNS Firewall Advanced)

La soglia di confidenza per DNS Firewall Advanced. È necessario fornire questo valore quando si crea una regola DNS Firewall Advanced. I valori del livello di confidenza significano:

- Alto: rileva solo le minacce più comprovate con una bassa percentuale di falsi positivi.
- Medio: fornisce un equilibrio tra il rilevamento delle minacce e i falsi positivi.
- Basso: offre il più alto tasso di rilevamento delle minacce, ma aumenta anche i falsi positivi.

Per ulteriori informazioni, consulta Impostazioni delle regole in DNS Firewall.

Azione

Come si desidera che DNS Firewall gestisca una query DNS il cui nome di dominio corrisponde alle specifiche nell'elenco dei domini della regola. Per ulteriori informazioni, consulta Operazioni delle regole in DNS Firewall.

Priorità

Impostazione univoca di numeri interi positivi per la regola all'interno del gruppo di regole che determina l'ordine di elaborazione. DNS Firewall ispeziona le query DNS in base alle regole in un gruppo di regole a cominciare dall'impostazione di priorità più bassa a salire. È possibile modificare la priorità di una regola in qualsiasi momento, ad esempio per modificare l'ordine di elaborazione o creare spazio per altre regole.

Operazioni delle regole in DNS Firewall

Quando DNS Firewall trova una corrispondenza tra una query DNS e una specifica di dominio in una regola, applica l'operazione specificata nella regola alla query.

Sarà necessario specificare una delle seguenti opzioni in ogni regola creata:

- Allow: interrompe l'ispezione della query e consente di andare avanti. Non disponibile per DNS Firewall Advanced.
- Alert: interrompe l'ispezione della query, ne consente l'esecuzione e registra un avviso per la query nei log di Route 53 Resolver.
- Block: interrompe l'ispezione della query, ne impedisce l'accesso alla destinazione desiderata bloccandola e registra l'azione di blocco per la query nei log di di Route 53 Resolver.

  Rispondi con la risposta di blocco configurata, da quanto segue:

  - NODATA - Rispondi indicando che la query ha avuto esito positivo, ma non è disponibile alcuna risposta corrispondente.
  - NXDOMAIN: rispondi indicando che il nome di dominio incluso nella query non esiste.
  - OVERRIDE: fornisci una sostituzione personalizzata nella risposta. Questa opzione richiede le seguenti impostazioni aggiuntive:
    - Record value: il record DNS personalizzato da restituire in risposta alla query.
    - Record type: il tipo di record DNS. Ciò determina il formato del valore del record. Deve essere `CNAME`.

- Time to live in seconds: il periodo di tempo consigliato per il resolver DNS o il browser Web per memorizzare nella cache il record di sostituzione e utilizzarlo in risposta a questa query, se viene ricevuto nuovamente. Per impostazione predefinita, questo è zero e il record non è memorizzato nella cache.

Per ulteriori informazioni sulla configurazione dei log delle query e sul contenuto, consulta Registrazione delle query di Resolver e Valori che vengono visualizzati nei log di query di Resolver.

Utilizzo Alert per testare le regole di blocco

La prima volta che crei una regola di blocco, puoi testarla configurandola con l'azione impostata su AlertÈ quindi possibile esaminare il numero di query per cui la regola invia un avviso per vedere quante query sarebbero bloccate se si imposta l'operazione su . Block.

Gestione di gruppi di regole e regole in DNS Firewall

Per gestire i gruppi di regole e le regole nella console, segui le indicazioni in questa sezione.

Quando si apportano modifiche alle entità DNS Firewall, ad esempio regole ed elenchi di domini, DNS Firewall propaga le modifiche ovunque le entità sono memorizzate e utilizzate. Le modifiche vengono applicate in pochi secondi, ma potrebbe esserci un breve periodo di incoerenza tra quando le modifiche sono arrivate in alcuni punti e non ancora in altri. Ad esempio, se si aggiunge un dominio a un elenco di domini a cui fa riferimento una regola di blocco, il nuovo dominio potrebbe essere bloccato brevemente in un'area del VPC mentre è ancora consentito in un'altra. Questa incoerenza temporanea può verificarsi quando si configura per la prima volta il gruppo di regole e le associazioni VPC e quando si modificano le impostazioni esistenti. Di solito, eventuali incoerenze di questo tipo durano solo pochi secondi.

Creazione di gruppi di regole e regole

Per creare un gruppo di regole e aggiungervi regole, segui i passaggi di questa procedura.

Come creare un gruppo di regole e le relative regole

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 3.

- O -

Accedi a AWS Management Console e apri il

la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/

2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Scegli Aggiungi gruppo di regole, quindi segui le istruzioni della procedura guidata per specificare il gruppo di regole e le impostazioni delle regole.

   Per informazioni sui valori per i gruppi di regole, consulta Impostazioni del gruppo di regole in DNS Firewall.

   Per informazioni sui valori per le regole, consulta Impostazioni delle regole in DNS Firewall.

Visualizzazione e aggiornamento di un gruppo di regole e di regole

Utilizza la seguente procedura per visualizzare i gruppi di regole e le regole loro assegnate. È inoltre possibile aggiornare il gruppo di regole e le impostazioni delle regole.

Come visualizzare e aggiornare un gruppo di regole

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 3.

   - O -

   Accedi a AWS Management Console e apri il

   la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/
2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Seleziona il gruppo di regole che desideri visualizzare o modificare, quindi scegli Visualizza dettagli.
5. Nella pagina del gruppo di regole è possibile visualizzare e modificare le impostazioni.

Per informazioni sui valori per i gruppi di regole, consulta Impostazioni del gruppo di regole in DNS Firewall.

Per informazioni sui valori per le regole, consulta Impostazioni delle regole in DNS Firewall.

Eliminazione di un gruppo di regole

Per eliminare un gruppo di regole, completa la seguente procedura.

> **Important**
>
> Se elimini un gruppo di regole associato a un VPC, DNS Firewall rimuove l'associazione e interrompe le protezioni fornite dal gruppo di regole al VPC.

Eliminazione delle entità DNS Firewall

Quando si elimina un'entità che è possibile utilizzare in DNS Firewall, ad esempio un elenco di domini che potrebbe essere in uso in un gruppo di regole o un gruppo di regole che potrebbe essere associato a un VPC, DNS Firewall verifica se l'entità è attualmente in uso. Se rileva che è in uso, DNS Firewall avvisa l'utente. DNS Firewall è quasi sempre in grado di determinare se un'entità è in uso. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Per essere certo che l'entità non sia utilizzata, controlla nelle configurazioni DNS Firewall prima di eliminarla. Se l'entità è un elenco di domini di riferimento, verifica che nessun gruppo di regole la stia utilizzando. Se l'entità è un gruppo di regole, verifica che non sia associata a nessuno VPCs.

Per eliminare un gruppo di regole

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 3.

   - O -

   Accedi a AWS Management Console e apri il

   la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/

2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Seleziona il gruppo di regole da eliminare, quindi scegli Elimina e conferma l'eliminazione.

Elenchi di domini di DNS Firewall per Route 53 Resolver

Un elenco di domini è un insieme riutilizzabile di specifiche di dominio utilizzate in una regola DNS Firewall all'interno di un gruppo di regole. Quando associ un gruppo di regole a un VPC, DNS Firewall confronta le query DNS con gli elenchi di dominio utilizzati nelle regole. Se trova una corrispondenza, la query DNS viene gestita in base all'operazione della regola corrispondente. Per ulteriori informazioni sui gruppi di regole e sulle regole, consulta Gruppi di regole e regole in DNS Firewall.

Gli elenchi di domini consentono di separare le specifiche esplicite del dominio dalle operazioni che si desidera eseguire su di essi. È possibile utilizzare un singolo elenco di domini in più regole e tutti gli aggiornamenti apportati all'elenco di domini influiranno automaticamente su tutte le regole che lo utilizzano.

Gli elenchi di domini rientrano in due categorie principali:

- elenchi di domini gestiti, che AWS creano e gestiscono per te.
- Elenchi di domini personalizzati, creati e gestiti da te.

In questa sezione vengono descritti i tipi di elenchi di domini gestiti disponibili e sono fornite le linee guida per la creazione e la gestione dei propri elenchi di domini, se si sceglie di farlo.

Elenchi di domini gestiti

Gli elenchi di domini gestiti contengono nomi di dominio associati ad attività dannose o altre potenziali minacce. AWS gestisce questi elenchi per consentire ai clienti di Route 53 Resolver di confrontare gratuitamente le query DNS in uscita quando utilizzano DNS Firewall.

Mantenersi aggiornati sul panorama delle minacce in continua evoluzione può essere dispendioso in termini di tempo e denaro. Gli elenchi di domini gestiti possono farti risparmiare tempo quando implementi e utilizzi DNS Firewall. AWS aggiorna automaticamente gli elenchi quando emergono nuove vulnerabilità e minacce. AWS riceve spesso notifiche in merito a nuove vulnerabilità prima

della divulgazione pubblica, quindi DNS Firewall può implementare misure di mitigazione per voi spesso prima che una nuova minaccia diventi nota a tutti.

Gli elenchi di domini gestiti sono progettati per aiutarti a proteggerti dalle minacce Web comuni e aggiungono un altro livello di sicurezza alle applicazioni. Gli elenchi di domini AWS gestiti traggono i dati sia da AWS fonti interne che da fonti interne e vengono continuamente RecordedFutureaggiornati. Tuttavia, gli elenchi di domini AWS gestiti non sono intesi come sostituti di altri controlli di sicurezza Amazon GuardDuty, ad esempio quelli determinati dalle AWS risorse selezionate.

Come procedura consigliata, prima di utilizzare un elenco di domini gestiti in produzione, verificarlo in un ambiente non di produzione, con l'azione della regola impostata su `Alert`. Valuta la regola utilizzando i CloudWatch parametri di Amazon combinati con le richieste campionate di Route 53 Resolver DNS Firewall o i log DNS Firewall. Quando sei certo che la regola esegue ciò che desideri, modifica l'impostazione dell'operazione in base alle necessità.

Elenchi di domini gestiti disponibili AWS

In questa sezione vengono descritti gli elenchi di domini gestiti attualmente disponibili. Quando ti trovi in una regione in cui sono supportati tali elenchi, li visualizzi sulla console quando gestisci gli elenchi di domini e quando specifichi l'elenco di domini per una regola. Nei log, l'elenco dei domini viene registrato all'interno del `firewall_domain_list_id field`.

AWS fornisce i seguenti elenchi di domini gestiti, nelle regioni in cui sono disponibili, per tutti gli utenti di Route 53 Resolver DNS Firewall.

- `AWSManagedDomainsMalwareDomainList`: i domini associati all'invio di malware, all'hosting di malware o alla distribuzione di malware.
- `AWSManagedDomainsBotnetCommandandControl`: i domini associati al controllo delle reti di computer infettati da malware spam.
- `AWSManagedDomainsAggregateThreatList`— Domini associati a diverse categorie di minacce DNS tra cui malware, ransomware, botnet, spyware e tunneling DNS per aiutare a bloccare diversi tipi di minacce. `AWSManagedDomainsAggregateThreatList`include tutti i domini negli altri elenchi di domini gestiti elencati qui. AWS
- `AWSManagedDomainsAmazonGuardDutyThreatList`— Domini associati ai risultati di sicurezza di Amazon GuardDuty DNS. I domini provengono esclusivamente dai sistemi di intelligence sulle minacce GuardDuty dell'azienda e non contengono domini provenienti da fonti esterne di terze parti. Più specificamente, attualmente questo elenco bloccherà solo i domini generati

internamente e utilizzati per i seguenti rilevamenti in: Impact: .Reputation. GuardDuty EC2/AbusedDomainRequest.Reputation, Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation, Impact:Runtime/AbusedDomainRequest.Reputation, Impact:Runtime/BitcoinDomainRequest.Reputation, and Impact:Runtime/MaliciousDomainRequest

Per ulteriori informazioni, consulta Finding types in the Amazon GuardDuty User Guide.

AWS Gli elenchi di domini gestiti non possono essere scaricati o sfogliati. Per proteggere la proprietà intellettuale, non è possibile visualizzare o modificare le specifiche dei singoli domini all'interno di un elenco di domini AWS gestiti. Questa restrizione consente anche di impedire agli utenti malintenzionati di pianificare minacce che possano eludere in modo specifico gli elenchi pubblicati.

Per testare gli elenchi di domini gestiti

Il seguente set di domini è fornito per testare gli elenchi di domini gestiti:

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 e AWSManaged DomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

Se non vengono bloccati, questi domini verranno risolti in 1.2.3.4. Se utilizzi gli elenchi di domini gestiti su un VPC, l'esecuzione di query per questi domini restituirà la risposta su cui è impostata un'azione di blocco nella regola (ad esempio NODATA).

Per ulteriori informazioni sugli elenchi di domini gestiti, contatta il Centro Supporto AWS.

La tabella seguente elenca la disponibilità delle regioni per gli elenchi di domini AWS gestiti.

Disponibilità delle regioni per gli elenchi di domini gestiti

Regione	Sono disponibili elenchi di domini gestiti?
Africa (Città del Capo)	Sì
Asia Pacifico (Hong Kong)	Sì
Asia Pacific (Hyderabad)	Sì
Asia Pacifico (Giacarta)	Sì
Asia Pacifico (Malesia)	Sì
Asia Pacifico (Melbourne)	Sì
Asia Pacifico (Mumbai)	Sì
Regione Asia Pacifico (Osaka-Locale)	Sì
Asia Pacifico (Seul)	Sì
Asia Pacifico (Singapore)	Sì
Asia Pacifico (Sydney)	Sì
Asia Pacifico (Tokyo)	Sì
Regione Canada (Centrale)	Sì

Regione	Sono disponibili elenchi di domini gestiti?
Canada occidentale (Calgary)	Sì
Regione Europa (Francoforte)	Sì
Europa (Irlanda)	Sì
Regione Europa (Londra)	Sì
Europa (Milano)	Sì
Regione Europa (Parigi)	Sì
Europa (Spagna)	Sì
Europa (Stoccolma)	Sì
Europa (Zurigo)	Sì
Israele (Tel Aviv)	Sì
Medio Oriente (Bahrein)	Sì
Medio Oriente (Emirati Arabi Uniti)	Sì
Sud America (San Paolo)	Sì
Stati Uniti orientali (Virginia settentrionale)	Sì

Regione	Sono disponibili elenchi di domini gestiti?
Stati Uniti orientali (Ohio)	Sì
Stati Uniti occidentali (California settentrionale)	Sì
US West (Oregon)	Sì
Cina (Pechino)	Sì
Cina (Ningxia)	Sì
AWS GovCloud (US)	Sì

Ulteriori considerazioni sulla sicurezza

AWS Gli elenchi di domini gestiti sono progettati per aiutarti a proteggerti dalle minacce web più comuni. Se utilizzati in maniera conforme alla documentazione, questi elenchi aggiungono un altro livello di sicurezza alle applicazioni. Gli elenchi di domini gestiti, tuttavia, non sono concepiti in sostituzione di altri controlli di sicurezza, determinati dalle risorse AWS selezionate. Per garantire che le risorse in uso AWS siano adeguatamente protette, consulta la guida contenuta nel Modello di responsabilità condivisa.

Mitigazione degli scenari di falsi positivi

Se si verificano scenari di falsi positivi nelle regole che utilizzano elenchi di domini gestiti per bloccare le query, procedi come indicato di seguito:

1. Nei log del Resolver, identifica il gruppo di regole e l'elenco di domini gestiti che causano il falso positivo. A tale scopo, individua il log per la query che DNS Firewall sta bloccando, ma che si desidera consentire. Il record di log elenca il gruppo di regole, l'azione della regola e l'elenco di domini gestiti. Per ulteriori informazioni sui log, consulta Valori che vengono visualizzati nei log di query di Resolver.

2. Crea una nuova regola nel gruppo di regole che consenta esplicitamente la query bloccata. Quando crei la regola, puoi definire un elenco di domini personalizzato con la sola specifica del dominio che desideri consentire. Segui le istruzioni per la gestione dei gruppi di regole e delle regole riportate in Creazione di gruppi di regole e regole.
3. Assegna la priorità alla nuova regola all'interno del gruppo di regole in modo che venga eseguita prima della regola che utilizza l'elenco dei domini gestiti. A tale scopo, assegna alla nuova regola un'impostazione di priorità inferiore.

Dopo aver aggiornato il gruppo di regole, la nuova regola consentirà esplicitamente il nome di dominio che desideri consentire prima dell'esecuzione della regola di blocco.

Gestione degli elenchi di domini personalizzati

Puoi creare elenchi di domini personalizzati per specificare le categorie di dominio che non trovi nelle offerte degli elenchi di domini gestiti o che preferisci gestire autonomamente.

Oltre alle procedure descritte in questa sezione, nella console è possibile creare un elenco di domini nel contesto della gestione delle regole DNS Firewall per Route 53 Resolver quando si crea o si aggiorna una regola.

Ogni specifica di dominio nell'elenco di domini deve soddisfare i seguenti requisiti:

- Può opzionalmente iniziare con * (asterisco).
- Ad eccezione dell'asterisco iniziale facoltativo e di un punto come delimitatore tra etichette, deve contenere solo i seguenti caratteri: `A-Z`, `a-z`, `0-9`, `-`(trattino).
- La lunghezza deve essere compresa tra 1 e 255 caratteri.

Quando si apportano modifiche alle entità DNS Firewall, ad esempio regole ed elenchi di domini, DNS Firewall propaga le modifiche ovunque le entità sono memorizzate e utilizzate. Le modifiche vengono applicate in pochi secondi, ma potrebbe esserci un breve periodo di incoerenza tra quando le modifiche sono arrivate in alcuni punti e non ancora in altri. Ad esempio, se si aggiunge un dominio a un elenco di domini a cui fa riferimento una regola di blocco, il nuovo dominio potrebbe essere bloccato brevemente in un'area del VPC mentre è ancora consentito in un'altra. Questa incoerenza temporanea può verificarsi quando si configura per la prima volta il gruppo di regole e le associazioni VPC e quando si modificano le impostazioni esistenti. Di solito, eventuali incoerenze di questo tipo durano solo pochi secondi.

Test dell'elenco di domini prima di utilizzarlo in produzione

Come best practice, prima di utilizzare un elenco di domini in produzione, testarlo in un ambiente non di produzione, con l'operazione della regola impostata su `Alert`. Valuta la regola utilizzando i CloudWatch parametri di Amazon e i log Resolver. I log forniscono il nome dell'elenco di domini per tutti gli avvisi e le azioni di blocco. Una volta certo che l'elenco dei domini corrisponde alle query DNS nel modo desiderato, modifica l'impostazione dell'operazione della regola in base alle esigenze. Per informazioni sulle CloudWatch metriche e sui log delle query, consulta, e. Monitoraggio dei gruppi di regole del firewall DNS di Route 53 Resolver con Amazon CloudWatch Valori che vengono visualizzati nei log di query di Resolver Gestione delle configurazioni di registrazione delle query di Resolver

Come aggiungere un elenco di domini

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC. Continua alla fase 2.

   - O -

   Accedi a AWS Management Console e apri il

   la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/
2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Elenchi di dominio. Nella pagina Elenchi di domini puoi selezionare e modificare gli elenchi di domini esistenti ed aggiungerne di tuoi.
3. Per aggiungere un elenco di domini, scegli Aggiungi elenco di domini.
4. Specifica un nome per l'elenco di domini, quindi immetti le specifiche del dominio nella casella di testo, una per riga.

   Se imposti Passa al caricamento in blocco su on, inserisci l'URI del bucket Amazon S3 in cui hai creato un elenco di domini. Questo elenco di domini deve avere un nome di dominio per riga.

   > **Note**
   >
   > I nomi di dominio duplicati impediranno l'importazione in blocco.
5. Scegli Aggiungi elenco di domini. La pagina Elenchi di domini riporta il nuovo elenco di domini.

Dopo aver creato l'elenco dei domini, sarà possibile farvi riferimento in base al nome dalle regole DNS Firewall.

Eliminazione delle entità DNS Firewall

Quando si elimina un'entità che è possibile utilizzare in DNS Firewall, ad esempio un elenco di domini che potrebbe essere in uso in un gruppo di regole o un gruppo di regole che potrebbe essere associato a un VPC, DNS Firewall verifica se l'entità è attualmente in uso. Se rileva che è in uso, DNS Firewall avvisa l'utente. DNS Firewall è quasi sempre in grado di determinare se un'entità è in uso. Tuttavia, in rari casi, potrebbe non essere in grado di farlo. Per essere certo che l'entità non sia utilizzata, controlla nelle configurazioni DNS Firewall prima di eliminarla. Se l'entità è un elenco di domini di riferimento, verifica che nessun gruppo di regole la stia utilizzando. Se l'entità è un gruppo di regole, verifica che non sia associata a nessuno. VPCs

Come eliminare un elenco di domini

1. Nel pannello di navigazione, scegli Elenchi di domini.
2. Nella barra di navigazione, sceglie la regione per l'elenco di domini.
3. Seleziona l'elenco di domini che desideri eliminare, quindi scegli Elimina e conferma l'eliminazione.

Route 53 Resolver DNS Firewall avanzato

DNS Firewall Advanced rileva le query DNS sospette sulla base di firme di minacce note nelle query DNS. È possibile specificare un tipo di minaccia in una regola utilizzata in una regola del firewall DNS, all'interno di un gruppo di regole. Quando associ un gruppo di regole a un VPC, DNS Firewall confronta le tue query DNS con i domini contrassegnati nelle regole. Se trova una corrispondenza, la query DNS viene gestita in base all'operazione della regola corrispondente.

DNS Firewall Advanced funziona identificando le firme di minacce DNS sospette ispezionando una serie di identificatori chiave nel payload DNS, tra cui il timestamp delle richieste, la frequenza delle richieste e delle risposte, le stringhe di query DNS e la lunghezza, il tipo o la dimensione delle query DNS in uscita e in entrata. In base al tipo di firma della minaccia, è possibile configurare politiche di blocco o semplicemente registrare e inviare avvisi sulla query. Utilizzando un set esteso di identificatori di minacce, è possibile proteggersi dalle minacce DNS provenienti da fonti di dominio che potrebbero non essere ancora classificate dai feed di intelligence sulle minacce gestiti dalla più ampia comunità di sicurezza.

Attualmente, DNS Firewall Advanced offre protezioni da:

- Algoritmi di generazione di domini () DGAs

  DGAs vengono utilizzati dagli aggressori per generare un gran numero di domini per lanciare attacchi di malware.

- tunneling DNS

  Il tunneling DNS viene utilizzato dagli aggressori per esfiltrare dati dal client utilizzando il tunnel DNS senza stabilire una connessione di rete con il client.

Per informazioni su come creare regole, consulta e. Creazione di gruppi di regole e regole Impostazioni delle regole in DNS Firewall

Configurazione della registrazione per DNS Firewall

Puoi valutare le regole del tuo firewall DNS utilizzando i CloudWatch parametri di Amazon e i log delle query Resolver. I log forniscono il nome dell'elenco di domini per tutti gli avvisi e le azioni di blocco. Per ulteriori informazioni su Amazon CloudWatch, consultaMonitoraggio dei gruppi di regole del firewall DNS di Route 53 Resolver con Amazon CloudWatch.

Quando abiliti DNS Firewall, lo associ a un VPC e hai la registrazione abilitata, `firewall_rule_group_id`, `firewall_rule_action` e `firewall_domain_list_id` sono i campi specifici del DNS Firewall forniti all'interno dei log.

> **Note**
>
> I log delle query mostreranno i campi del DNS Firewall aggiuntivi solo per le query bloccate dalle regole del DNS Firewall.

Per iniziare a registrare le query DNS filtrate in base alle regole del firewall DNS che hanno origine nel tuo VPCs, esegui le seguenti attività nella console Amazon Route 53:

Come configurare la registrazione delle query del Resolver per DNS Firewall

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/

2. Espandi il menu della console Route 53. Nell'angolo in alto a sinistra della console, scegli l'icona con le tre barre orizzontali ().
3. Nel menu Resolver, scegli Registrazione delle query.
4. Nel selettore Regione, scegli la AWS regione in cui desideri creare la configurazione di registrazione delle interrogazioni.

   Questa deve essere la stessa regione in cui hai creato VPCs quella associata al firewall DNS per cui desideri registrare le query. Se ci si trova VPCs in più regioni, è necessario creare almeno una configurazione di registrazione delle query per ogni regione.
5. Scegli Configura registrazione delle query.
6. Specifica i seguenti valori:

   Nome della configurazione della registrazione delle query

   Specifica un nome per la configurazione della registrazione delle query. Il nome sarà visualizzato nella console nell'elenco delle configurazioni di registrazione delle query. Specifica un nome che consenta di trovare facilmente questa configurazione in un secondo momento.

   Destinazione dei log delle query

   Scegli il tipo di AWS risorsa a cui desideri che Resolver invii i log delle query. Per informazioni su come scegliere tra le opzioni (CloudWatch Logs log group, S3 bucket e Firehose delivery stream), consulta. AWS risorse a cui puoi inviare i log delle query di Resolver

   Dopo aver scelto il tipo di risorsa, puoi creare un'altra risorsa di quel tipo o scegliere una risorsa esistente creata dall'account corrente. AWS

   > **Note**
   >
   > È possibile scegliere solo le risorse che sono state create nella regione AWS scelta nella fase 4, la regione in cui si sta creando la configurazione di registrazione delle query. Se decidi di creare una nuova risorsa, tale risorsa verrà creata nella stessa regione.

VPCs per registrare le interrogazioni per

Questa configurazione di registrazione delle query registrerà le query DNS che hanno origine nel server scelto dall' VPCs utente. Seleziona la casella di controllo relativa a ciascun VPC nella regione corrente per cui desideri che il Resolver record le query, quindi seleziona Scegli.

> **Note**
>
> Il recapito dei log VPC può essere abilitato una sola volta per un tipo di destinazione specifico. I log non possono essere recapitati a più destinazioni dello stesso tipo. Ad esempio, i log VPC non possono essere consegnati a due destinazioni Amazon S3.

7. Scegli Configura registrazione delle query.

> **Note**
>
> Le query DNS eseguite dalle risorse nel VPC vengono visualizzate nei log dopo pochi minuti dalla creazione della configurazione della registrazione delle query.

Condivisione dei gruppi di regole del firewall DNS di Route 53 Resolver tra account AWS

È possibile condividere i gruppi di regole DNS Firewall tra account. AWS Per condividere i gruppi di regole, si usa AWS Resource Access Manager (AWS RAM). La console DNS Firewall si integra con la AWS RAM console. Per ulteriori informazioni AWS RAM, consultare la Guida per l'utente di Resource Access Manager.

Tieni presente quanto segue:

Associazione di gruppi di regole condivisi con VPCs

Se un altro AWS account ha condiviso un gruppo di regole con il tuo account, puoi associarlo VPCs allo stesso modo in cui associ i gruppi di regole che hai creato. Per ulteriori informazioni, consulta Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver.

Eliminazione o annullamento della condivisione di un gruppo di regole condiviso

Se condividi un gruppo di regole con altri account e poi elimini il gruppo di regole o interrompi la condivisione, DNS Firewall rimuove tutte le associazioni create dagli altri account tra il gruppo di regole e i loro VPCs.

Impostazioni massime per gruppi di regole e associazioni

I gruppi di regole condivisi e le relative associazioni VPCs sono inclusi nei conteggi degli account con cui vengono condivisi i gruppi di regole.

Per le quote correnti di DNS Firewall, consulta Quote su DNS Firewall per Route 53 Resolver.

Autorizzazioni

Per condividere un gruppo di regole con un altro AWS account, è necessario disporre dell'autorizzazione per utilizzare l'PutFirewallRuleGroupPolicyazione.

Restrizioni sull' AWS account con cui è condiviso un gruppo di regole

L'account con cui si condivide un gruppo di regole non può modificare né eliminare il gruppo.

Assegnazione di tag

Solo l'account che ha creato un gruppo di regole può aggiungere, eliminare o visualizzare i tag sul gruppo di regole.

Per visualizzare lo stato di condivisione corrente di un gruppo di regole (incluso l'account che ha condiviso il gruppo di regole o l'account con cui il gruppo di regole è condiviso) e per condividere i gruppi di regole con un altro account, completa la seguente procedura.

Per visualizzare lo stato di condivisione e condividere i gruppi di regole con un altro AWS account

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegliere Rule groups (Gruppi di regole).
3. Nella barra di navigazione, seleziona la regione dove è stato creato il gruppo di regole.

   La colonna Stato condivisione mostra lo stato corrente dei gruppi di regole creati dall'account attuale o condivisi con l'account attuale.

   - Non condiviso: l' AWS account corrente ha creato il gruppo di regole e il gruppo di regole non è condiviso con altri account.

- Condiviso da me: l'account corrente ha creato il gruppo di regole e l'ha condiviso con uno o più account.
- Condiviso con me: un altro account ha creato il gruppo di regole e l'ha condiviso con l'account corrente.

4. Scegli il nome del gruppo di regole di cui si desidera visualizzare le informazioni di condivisione o che si desidera condividere con un altro account.

   Nella *rule group name* pagina Gruppo di regole:, il valore in Proprietario mostra l'ID dell'account che ha creato il gruppo di regole. Questo è l'account attuale, a meno che il valore di Sharing status (Stato di condivisione) non sia Shared with me (Condivisa con me). In questo caso, il Proprietario è l'account che ha creato il gruppo di regole e l'ha condiviso con l'account corrente.

5. Seleziona Condividi per visualizzare ulteriori informazioni o per condividere il gruppo di regole con un altro account. Viene visualizzata una pagina nella AWS RAM console, a seconda del valore dello stato di condivisione:

   - Non condivisa: viene visualizzata la pagina Create resource share (Crea condivisione risorsa). Per ulteriori informazioni su come condividere il gruppo di regole con un altro account, unità organizzativa (UO) o organizzazione, continua con la fase successiva.
   - Condiviso da me: la pagina Risorse condivise riporta i gruppi di regole e le altre risorse di proprietà dell'account corrente e condivisi con altri account.
   - Condiviso con me: la pagina Risorse condivise mostra i gruppi di regole e le altre risorse di proprietà di altri account e condivisi con l'account corrente.

6. Per condividere un gruppo di regole con un altro AWS account, unità organizzativa o organizzazione, specifica i seguenti valori.

   > **Note**
   >
   > Non è possibile aggiornare le impostazioni di condivisione. Per modificare una delle seguenti impostazioni, devi ricondividere un gruppo di regole con le nuove impostazioni e rimuovere le precedenti impostazioni di condivisione.

   Descrizione

   Inserisci una breve descrizione che ti aiuti a ricordare perché hai condiviso il gruppo di regole.

Risorse

Seleziona la casella di controllo del gruppo di regole che desideri condividere.

Principali

Inserire il numero di AWS account, il nome dell'unità organizzativa o il nome dell'organizzazione.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS fattura; è possibile utilizzare anche i tag per altri scopi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Abilitazione delle protezioni DNS Firewall per Route 53 Resolver per il VPC

È possibile abilitare le protezioni di DNS Firewall per il VPC associando uno o più gruppi di regole al VPC. Ogni volta che un VPC viene associato a un gruppo di regole di DNS Firewall, Route 53 Resolver fornisce le seguenti protezioni:

- Il Resolver instrada le query DNS in uscita del VPC tramite DNS Firewall e DNS Firewall filtra le query utilizzando i gruppi di regole associati.
- Il Resolver applica le impostazioni nella configurazione di DNS Firewall del VPC.

Per fornire le protezioni di DNS Firewall al VPC, completa le seguenti operazioni:

- Crea e gestisci le associazioni tra i gruppi di regole di DNS Firewall e il VPC. Per informazioni sui gruppi di regole, consulta Gruppi di regole e regole in DNS Firewall.
- Configura come desideri che Resolver gestisca le query DNS per il VPC durante un errore, ad esempio se DNS Firewall non fornisce una risposta per una query DNS.

Gestione delle associazioni tra il VPC e il gruppo di regole DNS Firewall per Route 53 Resolver

Come visualizzare le associazioni VPC di un gruppo di regole

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   Nel pannello di navigazione seleziona Firewall DNS per aprire la pagina dei Gruppi di regole del Firewall DNS sulla console Amazon VPC.

   - O -

   Accedi a AWS Management Console e apri il

   la console Amazon VPC sotto. https://console.aws.amazon.com/vpc/
2. Nel pannello di navigazione, sotto la voce Firewall DNS seleziona Gruppi di regole.
3. Nella barra di navigazione, scegli la regione per il gruppo di regole.
4. Seleziona il gruppo di regole da associare.
5. Seleziona Visualizza dettagli. Viene visualizzata la pagina Gruppo di regole.
6. Nella parte inferiore, puoi vedere un'area con i dettagli a schede che include regole e informazioni associate. VPCs Scegli la scheda Associato. VPCs

Come associare un gruppo di regole a un VPC

1. Individua le associazioni VPC del gruppo di regole seguendo le istruzioni riportate nella procedura precedente Come visualizzare le associazioni VPC di un gruppo di regole.
2. Nella VPCs scheda Associato, scegli Associa VPC.
3. Nel menu a discesa individua il VPC che intendi associare al gruppo di regole. Selezionalo, quindi scegli Associa.

Nella pagina del gruppo di regole, il tuo VPC è elencato nella scheda VPCsAssociato. In un primo momento, lo Stato dell'associazione riporta Aggiornamento in corso. Al termine dell'associazione, lo stato diventa Completo.

Come rimuovere un'associazione tra un gruppo di regole e un VPC

1. Individua le associazioni VPC del gruppo di regole seguendo le istruzioni riportate nella procedura precedente Come visualizzare le associazioni VPC di un gruppo di regole.
2. Seleziona il VPC che desideri rimuovere dall'elenco, quindi scegli Dissocia. Verifica, quindi conferma l'operazione.

Nella pagina del gruppo di regole, il tuo VPC è elencato nella VPCs scheda Associato con lo stato di Dissociazione. Al termine dell'operazione, DNS Firewall aggiornerà l'elenco in modo da rimuovere il VPC.

Configurazione del VPC di DNS Firewall

La configurazione DNS Firewall per il VPC determina se Route 53 Resolver consente le query o le blocca durante gli errori, ad esempio quando DNS Firewall è compromesso, non risponde o non è disponibile nella zona. Il Resolver applica la configurazione del firewall di un VPC ogni volta che al VPC sono associati uno o più gruppi di regole di DNS Firewall.

È possibile configurare un VPC in modo che non venga aperto o chiuso.

- Per impostazione predefinita, la modalità di errore è chiusa, il che significa che Resolver blocca tutte le query per le quali non riceve una risposta da DNS Firewall e invia una risposta DNS `SERVFAIL`. Questo approccio favorisce la sicurezza rispetto alla disponibilità.
- Se si attiva l'errore di apertura, Resolver consente di eseguire le query se non riceve una risposta da DNS Firewall. Questo approccio favorisce la disponibilità rispetto alla sicurezza.

Come modificare la configurazione di DNS Firewall per un VPC (console)

1. Accedi AWS Management Console e apri la console Resolver all'indirizzo. https://console.aws.amazon.com/route53resolver/
2. Nel riquadro di navigazione sotto Resolvers, scegli. VPCs
3. Nella VPCspagina, individua e modifica il VPC. Modifica la configurazione di DNS Firewall in modo che non venga aperto o chiuso in base alle esigenze.

Come modificare il comportamento di DNS Firewall per un VPC (API)

- Aggiorna la configurazione del firewall VPC chiamando UpdateFirewallConfige abilitando o disabilitando. `FirewallFailOpen`

Puoi recuperare un elenco delle configurazioni del firewall VPC tramite l'API chiamando. ListFirewallConfigs

Cosa sono i profili Amazon Route 53?

Con Route 53 Profiles, puoi applicare e gestire configurazioni Route 53 relative al DNS su molte VPCs e diverse configurazioni. Account AWS I profili semplificano la gestione delle impostazioni DNS per molti VPCs utenti tanto quanto la gestione di un singolo VPC e quando si aggiorna un profilo, le sue impostazioni vengono propagate a tutti i profili associati VPCs al profilo. Puoi anche condividere un profilo con le Account AWS stesse regioni utilizzando. AWS RAM Le risorse attualmente supportate da Route 53 che puoi associare a un profilo sono:

- Zone ospitate private e impostazioni in esse specificate.
- Regole di Route 53 Resolver, sia di inoltro che di sistema.
- Gruppi di regole DNS Firewall.

Alcune configurazioni VPC sono gestite direttamente sul profilo. Le configurazioni sono:

- Configurazione di ricerca DNS inversa per Resolver Rules.
- Configurazione della modalità di errore del firewall DNS.
- Configurazione di convalida DNSSEC.

Ad esempio, puoi abilitare la configurazione della modalità di errore del firewall DNS per tutti i profili a cui è associato VPCs il profilo, ma mantenere la configurazione di convalida DNSSEC esistente del VPC.

> **Important**
>
> Dopo aver abilitato le impostazioni del profilo per le configurazioni precedenti e aver associato il profilo a un VPC, le impostazioni del profilo hanno effetto immediato.

È inoltre possibile utilizzarle AWS CloudFormation per configurare impostazioni DNS coerenti per i nuovi provisioning. VPCs

Puoi associare un profilo per VPC e il numero di risorse che puoi associare per profilo varia. Per ulteriori informazioni, consulta Quote sui profili della Route 53 .

Come viene assegnata la priorità alle impostazioni del profilo Route 53

È possibile impostare le impostazioni e le associazioni DNS locali per i profili per la migrazione o per altri scopi di test. Quando una query DNS soddisfa sia la regola Resolver per una zona ospitata privata direttamente associata al VPC sia una regola Resolver per una zona ospitata privata associata al profilo, le impostazioni DNS locali hanno la precedenza. Quando viene effettuata una query DNS per un nome di dominio in conflitto, vince quello più specifico. La tabella seguente include esempi dell'ordine di valutazione:

query DNS	Regola del profilo	Regola VPC	Regola valutata
esempio.com	esempio.com	esempio.com	VPC locale
test.example.com	test.example.com	esempio.com	Profilo
marketing.example.com	Nessuno	marketing.example.com	VPC locale

Route 53 Profiles Disponibilità regionale

Per visualizzare la disponibilità regionale e gli endpoint, consulta Endpoints di servizio per Route 53 nella guida di riferimento AWS generale.

Passaggi di alto livello per l'utilizzo dei profili Route 53

Per implementare i profili Amazon Route 53 nel tuo Amazon Virtual Private Cloud VPCs, esegui i seguenti passaggi di alto livello.

1. Crea un profilo vuoto: il primo passaggio consiste nel creare un profilo vuoto a cui associare risorse DNS. Per ulteriori informazioni, consulta Creazione di profili Route 53.
2. Associa le risorse DNS al profilo: le risorse che puoi attualmente associare a un profilo sono zone ospitate private, regole Route 53 Resolver, sia di inoltro che di sistema e gruppi di regole DNS Firewall. Per ulteriori informazioni, consulta,. Associare gruppi di regole DNS Firewall a un profilo

Route 53 Associare zone ospitate private a un profilo Route 53 Associa le regole del Resolver a un profilo Route 53

3. Configura alcune impostazioni VPC per il profilo: alcune impostazioni DNS, come le zone ospitate associate al profilo, vengono applicate immediatamente. VPCs Per le configurazioni della convalida DNSSEC, della ricerca DNS inversa di Resolver e della modalità di errore DNS Firewall, puoi scegliere una delle seguenti opzioni:
   - Per la convalida DNSSEC, puoi scegliere di utilizzare la configurazione VPC locale (impostazione predefinita), abilitare la convalida o disabilitare la convalida per tutti gli elementi associati al profilo. VPCs
   - Per la configurazione della ricerca DNS inversa di Resolver è possibile abilitarla, disabilitarla o utilizzare le regole definite automaticamente per il VPC localmente (impostazione predefinita).
   - Per la configurazione della modalità di errore DNS Firewall è possibile abilitarla, disabilitarla o utilizzare la configurazione della modalità di errore definita per il VPC localmente (impostazione predefinita).

   Per ulteriori informazioni, consulta Modifica le configurazioni del profilo della Route 53.
4. Associa il profilo a uno o più VPCs: per iniziare a utilizzare il tuo profilo, associalo a uno o più. VPCs Per ulteriori informazioni, consulta Associa un profilo Route 53 a VPCs.

Creazione di profili Route 53

Per creare profili Route 53, segui le indicazioni riportate in questo argomento. Scegli una scheda per creare un profilo Route 53 utilizzando la console Route 53, oppure AWS CLI.

- Console
- CLI

Console

Per creare un profilo Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Nella barra di navigazione, scegli la regione in cui desideri creare il profilo.

4. Inserisci un nome per il profilo, opzionalmente aggiungi dei tag e scegli Crea profilo.

   Questo crea un profilo vuoto con configurazioni predefinite a cui è possibile associare risorse. Dopo aver associato le risorse al profilo, è possibile associarlo a diverse VPCs e modificare il modo in cui alcune configurazioni del Resolver si applicano a. VPCs

CLI

È possibile creare un profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per. `name`

```
aws route53profiles create-profile --name test
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
    }
}
```

Per associare i tuoi profili a risorse diverse e modificare le configurazioni VPC per il profilo, consulta le seguenti procedure:

Argomenti

- Associare gruppi di regole DNS Firewall a un profilo Route 53
- Associare zone ospitate private a un profilo Route 53
- Associa le regole del Resolver a un profilo Route 53
- Modifica le configurazioni del profilo della Route 53

- Associa un profilo Route 53 a VPCs

Associare gruppi di regole DNS Firewall a un profilo Route 53

Scegli una scheda per associare i gruppi di regole DNS Firewall a un profilo Route 53 utilizzando la console Route 53, oppure AWS CLI.

- Console
- CLI

Console

Per associare i gruppi di regole DNS Firewall

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
3. Nel riquadro di navigazione, scegli Profili e nella tabella Profili, scegli il nome collegato del profilo con cui desideri lavorare.
4. Nella <Profile name>pagina, scegli la scheda Gruppi di regole DNS Firewall, quindi Associa.
5. Nella sezione Gruppi di regole DNS Firewall puoi selezionare fino a 10 gruppi di regole che hai creato in precedenza. Se desideri associare più di 10 gruppi di regole, usa il APIs. Per ulteriori informazioni, consulta AssociateResourceToProfile.

   Per creare nuovi gruppi di regole, consultaCreazione di gruppi di regole e regole.
6. Scegli Next (Successivo).
7. Nella pagina Definisci priorità è possibile impostare l'ordine in cui i gruppi di regole vengono elaborati facendo clic sul numero di priorità preassegnato e digitandone uno nuovo. I valori consentiti per la priorità sono compresi tra 100 e 9900.

   I gruppi di regole vengono valutati a partire dall'impostazione della priorità numerica più bassa e aumentando. È possibile modificare la priorità di un gruppo di regole in qualsiasi momento, ad esempio per modificare l'ordine di elaborazione o creare spazio per altri gruppi di regole.

   Scegli Invia.

8. L'avanzamento dell'associazione viene visualizzato nella colonna Stato della finestra di dialogo dei gruppi di regole DNS Firewall.

CLI

È possibile associare un gruppo di regole a un profilo eseguendo un AWS CLI comando come il seguente e utilizzando i propri valori per `name` `profile-id``resource-arn`, e`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}"
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
    }
}
```

Associare zone ospitate private a un profilo Route 53

Segui i passaggi di questa procedura per associare una zona ospitata privata a un profilo.

Per associare zone ospitate private

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
3. Nel riquadro di navigazione, scegli Profili e nella tabella Profili, scegli il nome collegato del profilo con cui desideri lavorare.
4. Nella <Profile name>pagina, scegli la scheda Zone ospitate private, quindi Associa.
5. Nella pagina Associa zone private ospitate puoi selezionare fino a 10 zone private ospitate che hai creato in precedenza. Se desideri associare più di 10 zone private ospitate, usa il APIs. Per ulteriori informazioni, consulta AssociateResourceToProfile.

   Per creare zone ospitate private, consultaCreazione di una zona ospitata privata.
6. Scegli Associa
7. L'avanzamento dell'associazione viene visualizzato nella colonna Stato della pagina Zone ospitate private.

Associa le regole del Resolver a un profilo Route 53

Segui i passaggi di questa procedura per associare le regole del Resolver a un profilo.

Per associare le regole Resolver

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
3. Nella pagina, scegli la scheda Regole del Resolver, quindi Associa. <Profile name>
4. Nella pagina delle regole del Resolver associato, nella tabella delle regole del Resolver è possibile selezionare fino a 10 regole del Resolver create in precedenza. Se si desidera associare più di 10 regole del resolver, utilizzare il. APIs Per ulteriori informazioni, consulta AssociateResourceToProfile.

   Per creare regole Resolver, vedi. Creazione delle regole di inoltro
5. Scegli Associa
6. L'avanzamento dell'associazione viene visualizzato nella colonna Stato della pagina delle regole del Resolver.

Modifica le configurazioni del profilo della Route 53

Dopo aver associato le risorse a un profilo, puoi modificare le configurazioni VPC predefinite per decidere come applicarle a. VPCs

Per modificare le configurazioni del profilo

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
3. Nel riquadro di navigazione, scegli Profili e nella tabella Profili, scegli il nome collegato del profilo con cui desideri lavorare.
4. Nella <Profile name>pagina, scegli la scheda Configurazione, quindi Modifica.
5. Nella pagina Modifica configurazione, scegli uno dei valori per la configurazione DNSSEC VPC, la configurazione di ricerca DNS inversa di Resolver e la configurazione della modalità di errore DNS Firewall.

   Per ulteriori informazioni sui valori, vedere. Impostazioni di configurazione per Route 53 Profile
6. Scegli Aggiorna.

Impostazioni di configurazione per Route 53 Profile

Quando si modifica una configurazione del profilo Route 53, si specificano i seguenti valori:

Configurazione DNSSEC

Seleziona uno dei seguenti valori:

- Usa la configurazione DNSSEC VPC locale (impostazione predefinita)

  Scegli questa opzione per fare in modo che tutti gli elementi VPCs associati a questo profilo mantengano la loro configurazione di convalida DNSSEC locale.
- Abilita la convalida DNSSEC

  Scegli questa opzione per abilitare la convalida DNSSEC in tutti i file associati a questo profilo. VPCs
- Disabilita la convalida DNSSEC

Scegli questa opzione per disabilitare la convalida DNSSEC in tutti gli elementi associati a VPCs questo profilo.

Configurazione della ricerca DNS inversa del Resolver

Seleziona uno dei seguenti valori:

- Attiva

  Scegli questa opzione per creare regole definite automaticamente per la ricerca DNS inversa in tutti i siti associati VPCs.

- Non abilitato

  Scegli questa opzione per non creare regole definite automaticamente per la ricerca DNS inversa in tutti i DNS associati VPCs.

- Usa regole locali definite automaticamente - impostazione predefinita

  Scegli questa opzione per utilizzare le impostazioni VPC locali per la ricerca DNS inversa del DNS associato. VPCs

Configurazione della modalità di errore del firewall DNS

Seleziona uno dei seguenti valori:

- Disabilita

  Scegli questa opzione per chiudere la modalità di errore del firewall DNS associata. VPCs Con questa opzione, DNS Firewall bloccherà tutte le query che non riesce a valutare correttamente.

- Enabled (Abilitato)

  Scegliete questa opzione per mantenere aperta la modalità di errore del firewall DNS per tutti i sistemi associati. VPCs Con questa opzione, DNS Firewall consentirà alle query di procedere se non è in grado di valutarle correttamente.

- Usa le impostazioni locali della modalità di errore (impostazione predefinita)

  Scegli questa opzione per utilizzare le impostazioni della modalità di errore del firewall DNS VPC locale.

Per ulteriori informazioni sulle configurazioni, vedere

- Abilitazione della convalida DNSSEC in Amazon Route 53

- Regole di inoltro per le query DNS inverse in Resolver
- Configurazione del VPC di DNS Firewall

Associa un profilo Route 53 a VPCs

Per associare un profilo Route 53 a un VPC, segui le indicazioni riportate in questo argomento. Scegli una scheda per associare un profilo Route 53 a un VPC utilizzando la console Route 53 oppure. AWS CLI

- Console
- CLI

Console

Associare VPCs

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
3. Nella <Profile name>pagina, scegli la VPCsscheda, quindi Associa.
4. Nella VPCs pagina Associa puoi selezionarne fino a 10 VPCs che hai creato in precedenza. Se vuoi associarne più di 10 VPCs, usa il APIs. Per ulteriori informazioni, consulta AssociateProfile.
5. Scegli Associa
6. L'avanzamento dell'associazione viene visualizzato nella colonna Stato della VPCspagina.

CLI

È possibile elencare i profili eseguendo un AWS CLI comando come il seguente e utilizzando i propri valori per `nameprofile-id`, `eresource-id`:

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
```

```
    "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"
    }
}
```

Visualizzazione e aggiornamento dei profili Amazon Route 53

Scegli la scheda della console per visualizzare e modificare il profilo della Route 53. Scegli la scheda CLI da utilizzare per AWS CLI elencare i profili che possiedi, condivisi da te o condivisi con te.

- Console
- CLI

Console

Visualizzazione e aggiornamento dei profili Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Seleziona il pulsante accanto al nome del profilo che desideri visualizzare o modificare.
4. Nella <Profile name>pagina è possibile visualizzare le risorse DNS attualmente associate, associarne di nuove e modificare i tag e le configurazioni VPC.

CLI

Puoi elencare i profili eseguendo un AWS CLI comando come il seguente:

```
aws route53profiles list-profiles
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

È possibile ottenere informazioni su un particolare VPS a cui è associato il profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per`profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
   "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"
    }   ]
}
```

Eliminazione di un profilo Amazon Route 53

Scegli una scheda per eliminare un profilo Route 53 utilizzando la console Route 53, oppure AWS CLI.

- Console
- CLI

Console

Per eliminare un profilo Route 53

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Seleziona il pulsante accanto al nome del profilo che desideri eliminare, quindi scegli Elimina.

> **Important**
>
> Non puoi eliminare un profilo se è associato a VPCs. Inoltre, se il profilo è condiviso con un altro Account AWS, qualsiasi configurazione a VPCs cui sono associate le configurazioni del profilo perderà tali configurazioni.

4. Nella finestra di dialogo Elimina, digitate**`confirm`**, quindi scegliete Elimina. <Profile name>

CLI

> **Important**
>
> Non puoi eliminare un profilo se è associato a VPCs. Inoltre, se il profilo è condiviso con un altro Account AWS, qualsiasi configurazione a VPCs cui sono associate le configurazioni del profilo perderà tali configurazioni.

È possibile eliminare un profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per: `profile-id`

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
    }
}
```

Visualizzazione e aggiornamento delle risorse Route 53 associate a un profilo Amazon Route 53

Scegli la scheda della console per visualizzare le associazioni di risorse del profilo Route 53 e, facoltativamente, modifica la priorità del gruppo di regole DNS Firewall. Scegli la scheda CLI da utilizzare per AWS CLI elencare le associazioni di risorse e per visualizzare un esempio di aggiornamento a una priorità di un gruppo di regole del firewall DNS.

- Console
- CLI

Console

Per visualizzare e aggiornare le risorse associate a un profilo

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.

4. Seleziona il pulsante accanto al nome del profilo per il quale desideri visualizzare o modificare le associazioni di risorse.
5. Nella **<Profile name>**pagina scegli la scheda relativa alla risorsa che desideri visualizzare o modificare, tra gruppi di regole del firewall DNS, zone ospitate private o regole Resolver.
6. Nella scheda di una risorsa è possibile visualizzare i nomi, l'ARN e lo stato delle risorse associate. Puoi anche scegliere l'icona a forma di ingranaggio per modificare ciò che viene visualizzato nella tabella delle risorse.

   Nella scheda Gruppi di regole DNS Firewall puoi anche scegliere la voce di priorità del gruppo di regole e modificarla con un numero più piccolo o più grande. I gruppi di regole vengono valutati in ordine a partire dal numero di priorità più bassa fino al numero di priorità più alta.

CLI

È possibile elencare le risorse associate a un profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per`profile-id`:

`aws route53profiles list-profile-resource-associations --profile-id` **`rp-4987774726example`**

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
        }
```

```
    ]
}
```

È possibile aggiornare la priorità di un gruppo di regole del firewall DNS associato a un profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per e utilizzando i propri valori per `profile-resource-association-id` e`--resource-properties`:

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
    }
}
```

Dissociazione di una risorsa da un profilo Amazon Route 53

Prima di eliminare un profilo, è necessario dissociare tutte le risorse da esso.

Per dissociare una risorsa associata a un profilo Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.

3. Nella barra di navigazione, scegli la regione in cui è stato creato il profilo da cui desideri dissociare una risorsa.
4. Selezionate il pulsante accanto al nome del profilo dal quale desiderate dissociare una risorsa.
5. Nella <Profile name>pagina scegli la scheda relativa alla risorsa che desideri eliminare, tra i gruppi di regole del firewall DNS, le zone ospitate private o le regole Resolver.
6. Nella scheda relativa alla risorsa, scegli la risorsa da cui desideri dissociare, quindi Dissocia.
7. Nella finestra di dialogo Dissocia risorse, digitate, quindi scegliete Dissocia**`confirm`**.

Visualizzazione VPCs associata a un profilo Amazon Route 53

Scegli la scheda della console per visualizzare e modificare le associazioni tra Route 53 Profile e VPC. Scegli la scheda CLI da utilizzare per AWS CLI elencare le associazioni da profilo a VPC o per ottenere informazioni su un'associazione specifica

- Console
- CLI

Console

Per visualizzare i dati VPCs associati a un profilo

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Nella barra di navigazione, scegli la regione in cui hai creato il profilo.
4. Seleziona il pulsante accanto al nome del profilo di cui desideri visualizzare il profilo associato VPCs.
5. Nella <Profile name>pagina scegli la VPCsscheda.
6. Nella scheda per VPCs è possibile visualizzare i nomi, l'ARN e lo stato degli associati. VPCs

CLI

È possibile elencare VPCs il profilo a cui è associato eseguendo un AWS CLI comando come il seguente:

```
aws route53profiles list-profile-associations
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
{
    "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"
        }
    ]
}
```

È possibile ottenere informazioni su un particolare VPS a cui è associato il profilo eseguendo un AWS CLI comando come il seguente e utilizzando il proprio valore per`profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id 
rpassoc-489ce212fexample
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
   "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"
    }   ]
}
```

Dissociazione di un VPC da un profilo Amazon Route 53

Scegli una scheda per dissociare un profilo Route 53 da un VPC utilizzando la console Route 53 oppure. AWS CLI

- Console
- CLI

Console

Per dissociare un VPC associato a un profilo Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione, scegli Profili.
3. Nella barra di navigazione, scegli la regione in cui è stato creato il profilo da cui desideri dissociare un VPC.
4. Seleziona il pulsante accanto al nome del profilo da cui desideri dissociare un VPC.
5. Nella <Profile name>pagina scegli la VPCsscheda.
6. VPCs Nella scheda della risorsa, scegli il VPC che desideri dissociare, quindi Dissocia.
7. Nella finestra di dialogo Dissocia risorse, digita, quindi scegli Dissocia**`confirm`**.

CLI

Puoi dissociare un profilo da un VPC eseguendo un AWS CLI comando come il seguente e utilizzando il tuo valore per e: `profile-id` `--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

Di seguito è riportato un esempio di output dopo l'esecuzione del comando:

```
"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"
    }
```

Utilizzo dei profili Route 53 condivisi

Puoi condividere un profilo con altri account nei seguenti modi:

- Concedere autorizzazioni di sola lettura, il che significa che l'altro account può associare il profilo al proprio. VPCs In questo caso tutte le risorse e le configurazioni DNS avranno effetto su quello associato. VPCs
- Concessione delle autorizzazioni di amministratore. In questo caso gli account con il profilo condiviso possono modificare il profilo e quindi associarlo al loro. VPCs Un proprietario può anche creare autorizzazioni gestite dal cliente che possono essere utilizzate per specificare quali azioni possono essere eseguite dall'account consumatore. Per ulteriori informazioni, consulta Autorizzazioni gestite dal cliente nella Guida per l'AWS RAM utente.

Amazon Route 53 Profile si integra con AWS Resource Access Manager (AWS RAM) per consentire la condivisione delle risorse. AWS RAM è un servizio che consente di condividere alcune risorse di Route 53 con altri Account AWS o tramite AWS Organizations. Con AWS RAM, condividi le risorse di

tua proprietà creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori includono:

- Specifico Account AWS
- Un'unità organizzativa all'interno della sua organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Questo argomento spiega come condividere le risorse che possiedi e come utilizzare le risorse condivise con te.

Indice

Concessione delle autorizzazioni per la condivisione dei profili Route 53

È richiesto un set minimo di autorizzazioni per consentire a un principale IAM di condividere un profilo. Ti consigliamo di utilizzare la policy IAM `AmazonRoute53ProfilesFullAccess` gestita per garantire che i tuoi responsabili IAM dispongano delle autorizzazioni necessarie per condividere e utilizzare i profili condivisi.

Se utilizzi una policy IAM personalizzata, sono necessarie le operazioni `route53profiles:GetProfilePolicy` e `route53profiles:PutProfilePolicy`. Si tratta di operazioni IAM che richiedono solo l'autorizzazione. Se a un preside IAM non vengono concesse queste autorizzazioni, si verificherà un errore durante il tentativo di condividere il profilo utilizzando il servizio. AWS RAM

Prerequisiti per la condivisione dei profili Route 53

- Per condividere un profilo Route 53, devi possederlo nel tuo Account AWS. Ciò significa che la risorsa deve essere allocata o fornita nel tuo account. Non puoi condividere un profilo Route 53 che è stato condiviso con te.
- Per condividere un profilo Route 53 con la propria organizzazione o un'unità organizzativa in AWS Organizations, è necessario abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Condivisione di un profilo Route 53

Quando condividi un profilo di tua proprietà con un altro Account AWS, consenti a quest'ultimo di applicare le impostazioni relative al DNS del profilo. VPCs Ciò semplifica l'applicazione di configurazioni DNS uniformi su migliaia di server VPCs con un sovraccarico di gestione minimo.

Per condividere un profilo Route 53, è necessario aggiungerlo a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che consente di condividere le risorse tra Account AWS. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi un profilo Route 53 utilizzando la console Route 53, lo aggiungi a una condivisione di risorse esistente. Per aggiungere il profilo Route 53 a una nuova condivisione di risorse, devi prima creare la condivisione di risorse utilizzando la AWS RAM console.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al profilo condiviso di Route 53. In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso al profilo condiviso della Route 53 dopo aver accettato l'invito.

Puoi iniziare a condividere un profilo Route 53 di tua proprietà sulla console Route 53 e continuare sulla AWS RAM console.

Per condividere un profilo Route 53 di tua proprietà utilizzando la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.

3. Seleziona il profilo che desideri condividere e nella pagina dei dettagli del profilo scegli Condividi profilo.
4. Verrai indirizzato alla AWS RAM console dove puoi seguire questi passaggi: Creazione di una condivisione di risorse nella Guida per l'AWS RAM utente.
5. Se un profilo è condiviso con te, la tabella Profili include il testo Condiviso con me.

   Quando hai condiviso un profilo, questo viene elencato come Condiviso nella tabella Profili.

Per condividere un profilo Route 53 di tua proprietà utilizzando la AWS RAM console

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere un profilo Route 53 di tua proprietà utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Annullamento della condivisione di un profilo Route 53 condiviso

Quando annulli la condivisione di un profilo e a VPCs cui sono associate le configurazioni di quel profilo, le perderai e verranno utilizzate per impostazione predefinita le configurazioni specifiche del VPC.

Per annullare la condivisione di un profilo Route 53 condiviso di tua proprietà, devi rimuoverlo dalla condivisione delle risorse. Puoi farlo utilizzando la console Route 53, la AWS RAM console o il AWS CLI.

Per annullare la condivisione di un profilo Route 53 condiviso di tua proprietà utilizzando la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Seleziona il nome collegato del profilo che desideri annullare la condivisione e, nella <Profile name>pagina, scegli Gestisci condivisione.
4. Verrai indirizzato alla AWS RAM console dove puoi seguire questi passaggi: Aggiornamento di una condivisione di risorse nella Guida per l'AWS RAM utente.

Per annullare la condivisione di un profilo Route 53 condiviso di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per annullare la condivisione di un profilo Route 53 condiviso di tua proprietà, utilizza il AWS CLI

Utilizza il comando disassociate-resource-share.

Identificazione di un profilo Route 53 condiviso

I proprietari e i consumatori possono identificare i profili Route 53 condivisi utilizzando la console Route 53 e AWS CLI.

Per identificare un profilo Route 53 condiviso utilizzando la console Route 53

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel riquadro di navigazione, scegli Profili.
3. Se un profilo è condiviso con te, la tabella Profili include il testo Condiviso con me.

   Quando hai condiviso un profilo, questo viene elencato come Condiviso nella tabella Profili.

Per identificare un profilo Route 53 condiviso utilizzando il AWS CLI

Utilizzate il comando get-profile o list-profile. I comandi restituiscono informazioni sui profili Route 53 di cui sei proprietario e sullo stato di condivisione dei profili Route 53.

Responsabilità e autorizzazioni per i profili Route 53 condivisi

Autorizzazioni per i proprietari

Il proprietario di un profilo può visualizzare, gestire ed eliminare le associazioni di risorse del profilo, comprese le associazioni di risorse create dagli account utente. Il proprietario è in grado di visualizzare ed eliminare le associazioni VPC di sua proprietà. Inoltre, solo il proprietario del profilo può eliminare un profilo di sua proprietà e ciò rimuove automaticamente tutte le associazioni di risorse del profilo.

Autorizzazioni per gli utenti

L'autorizzazione predefinita per i consumatori di un profilo condiviso è di sola lettura. Con l'autorizzazione di sola lettura possono vedere le risorse associate e associarle VPCs, ma non possono gestire le associazioni di risorse.

Un proprietario può anche creare autorizzazioni gestite dal cliente sulla console. AWS RAM Per ulteriori informazioni, consulta Creazione e utilizzo delle autorizzazioni gestite dal cliente nella Guida per l'AWS RAM utente.

Fatturazione e misurazione

I profili Route 53 vengono fatturati in base al numero di associazioni VPC. Il proprietario del profilo è responsabile della fattura per le associazioni VPC da parte del cliente.

Quote di istanze

I proprietari e i consumatori del profilo condividono la stessa quota, ad eccezione del numero di profili Route 53 per account in una regione. Per ulteriori informazioni, consulta Quote sui profili della Route 53

Che cos'è Amazon Route 53 on Outposts?

AWS Outposts è un servizio completamente gestito che estende AWS infrastrutture APIs, servizi e strumenti alle sedi dei clienti. Ciò consente ai clienti di eseguire AWS servizi con carichi di lavoro locali utilizzando le stesse interfacce di programmazione di. Regioni AWSPer ulteriori informazioni, consulta Cos'è? AWS Outposts nella Guida AWS Outposts per l'utente.

Route 53 on Outposts offre due funzionalità:

- Un Resolver che memorizza nella cache tutte le query DNS che provengono da AWS Outposts.
- Una connettività ibrida tra un Outpost e un resolver DNS on-premise quando metti in produzione endpoint in entrata e in uscita.

Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.

Inoltre, Route 53 on Outposts riduce la latenza di rete consentendo la risoluzione delle query all'interno dell'Outpost anziché effettuare il round-trip nella più vicina Regione AWS.

> **Note**
>
> Se disponi di una versione dei AWS Outposts rack non compatibile con Route 53 su Outposts, un team AWS dell'account riceverà una notifica e ti contatterà per aiutarti a effettuare l'upgrade. AWS Outposts

Caratteristiche di Amazon Route 53 on Outposts

La tabella seguente descrive le differenze tra le funzionalità di Route 53 on Outposts e quelle di Amazon Route 53.

Confronto tra Route 53 on Outposts e Route 53

Funzionalità	Disponibilità in Route 53 on Outposts
Route 53 Resolver	Sì. Resolver mantiene una cache locale di record per le applicazioni ospitate sul rack Outpost, il VPC peerizzat o in e qualsiasi nome host accessibile Regione AWS pubblicamente.

Funzionalità	Disponibilità in Route 53 on Outposts
Controlli dell'integrità	No. I controlli dell'integrità vengono calcolati e segnalati dalla Regione AWS. Se un Outpost si disconnette dal cloud, l'apertura degli endpoint non va a buon fine e non è possibile eseguire il failover su un backup.
Endpoint Resolver	Sì. Gli endpoint Resolver sul rack Outpost consentono di inoltrare e ricevere le query DNS dai server DNS on-premise. Per gli IPv4 endpoint è disponibile solo il tipo di endpoint.
DNS Firewall per Route 53 Resolver	Non disponibile.
Flusso di traffico	Non disponibile.

Comportamento del Resolver Route 53 quando AWS Outposts è disconnesso dal VPC

Se AWS Outposts è disconnesso da, il Resolver su Regione AWS Outpost si comporta come segue:

- Le modifiche sul piano di controllo (control-plane) non sono disponibili.
- I controlli dell'integrità e la funzionalità di failover DNS non sono disponibili.
- Le query DNS delle risorse ospitate localmente negli Outpost vengono risolte, ma in alcuni casi la risposta potrebbe essere obsoleta se l'indirizzo IP della risorsa è stato aggiornato mentre l'Outpost era disconnesso.
- Le query DNS delle risorse ospitate sul VPC della regione sono risolvibili. Tuttavia, le risorse non saranno accessibili finché non verrà ripristinata la connessione Outpost a. Regione AWS
- Le query DNS delle risorse DNS pubbliche possono essere risolte se sono disponibili nella cache di Route 53 Resolver su Outpost.

Nozioni di base su Route 53 Resolver in AWS Outposts

Dopo aver ordinato i AWS Outposts rack e averli consegnati, come descritto qui: Creane uno AWS Outposts nella AWS Outposts guida, puoi configurare Resolver su Outpost.

Puoi anche usarlo APIs per gestire Route 53 su Outposts. Per ulteriori informazioni consulta Operazioni Risolver su Outpost.

> **Important**
>
> Possono essere necessari fino a 30-150 minuti per creare una cache Resolver su un AWS Outposts.

Dopo la consegna degli AWS Outposts scaffali, puoi optare per Route 53 su Outposts.

Configurazione di Resolver su Outpost

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Nella pagina Resolver su Outpost, scegli Crea Resolver.
5. Nella pagina Crea Resolver:
   - In AWS Outpostsseleziona e su AWS Outposts cui vuoi creare il Resolver.
   - Digita un nome per il Resolver nella casella di testo Nome Resolver.
   - Dopo che i tipi di istanze consigliati per Resolver sono stati compilati con EC2 le istanze Amazon, scegline una.

     Per ulteriori informazioni sui tipi di istanza supportati, consulta Quote su Resolver su Outpost.
   - Alla voce Numero di istanze scegli il numero di istanze di interfaccia elastica per il VPC Resolver. Il valore predefinito è 4.

     Se AWS Outposts non disponi di un tipo di istanza che supporti Resolver, non potrai creare un Resolver.
6. Scegliere Create Resolver (Crea resolver).

   Puoi monitorare la creazione del Resolver nella pagina Resolver su Outpost.

Creazione di endpoint in entrata

Dopo aver creato un Resolver su Outpost, puoi aggiungere endpoint sia in entrata sia in uscita per risolvere le query DNS da e verso la tua rete on-premise.

Configurazione di endpoint in entrata per Resolver su Outpost

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Nella tabella Endpoint in entrata, seleziona Crea endpoint in entrata.
6. Nella pagina Crea servizio endpoint in entrata, inserisci i valori applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di endpoint in entrata su un Outpost.
7. Seleziona Crea endpoint.

Valori da specificare durante la creazione o la modifica di endpoint in entrata su un Outpost

Quando crei o modifichi un endpoint in entrata, devi specificare i seguenti valori:

ID Outpost

Se stai creando l'endpoint per un Resolver su un AWS Outposts VPC, questo è l'ID. AWS Outposts

Nome endpoint

Un nome descrittivo che ti consenta di trovare facilmente un endpoint in entrata nel pannello di controllo.

VPC nella regione region-name.

Tutte le query DNS in entrata dalla rete passano per questo VPC in direzione di Resolver.

Gruppo di sicurezza per questo endpoint

L'ID di uno o più gruppi di sicurezza che desideri utilizzare per controllare l'accesso a questo endpoint in uscita. Il gruppo di sicurezza specificato deve includere una o più regole in entrata. Le regole in entrata devono autorizzare l'accesso TCP e UDP sulla porta 53. Non puoi modificare questo valore dopo avere creato l'endpoint.

Per ulteriori informazioni, consulta Gruppi di sicurezza per il VPC nella Guida per l'utente di Amazon VPC.

Indcirizzi IP

Gli indirizzi IP a cui vuoi che i resolver DNS sulla rete inoltrino le query DNS. Richiediamo di specificare un minimo di due indirizzi IP per la ridondanza. Tieni presente quanto segue:

Indirizzi IP e interfacce di rete elastiche di Amazon VPC

Per ogni combinazione di zona di disponibilità, sottorete e indirizzo IP specificata, Resolver crea un'interfaccia di rete elastica di Amazon VPC. Per quanto riguarda il numero massimo di query DNS al secondo per ogni indirizzo IP in un endpoint, consulta Quote relative a Route 53 Resolver. Per informazioni sui prezzi per ogni interfaccia di rete elastica, consulta Amazon Route 53 nella Pagina dei prezzi di Amazon Route 53.

> **Note**
>
> L'endpoint del risolutore ha un indirizzo IP privato. Questi indirizzi IP non cambieranno nel corso della vita di un endpoint.

Per ogni indirizzo IP, specifica i seguenti valori. Ogni indirizzo IP deve trovarsi in una zona di disponibilità del VPC specificato in VPC in the region-name Region (VPC nella regione region-name).

Zona di disponibilità

La zona di disponibilità nella quale desideri che le query DNS passino in direzione del VPC. La zona di disponibilità specificata deve essere configurata con una sottorete.

Sottorete

La sottorete contenente l'indirizzo IP a cui si desidera inoltrare le query DNS. La sottorete deve avere a disposizione un indirizzo IP.

Specificare la sottorete per un indirizzo. IPv4 IPv6 non è supportata.

Indirizzo IP

L'indirizzo IP al quale desideri inoltrare le query DNS.

Scegli se vuoi che sia Resolver a scegliere un indirizzo IP per tuo conto tra gli indirizzi IP disponibili nella sottorete specificata o se vuoi specificare personalmente l'indirizzo IP.

Se scegli di specificare tu stesso l'indirizzo IP, inserisci un IPv4 indirizzo. IPv6 non è supportato.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS fattura; è possibile utilizzare i tag anche per altri scopi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Creazione di endpoint in uscita

Dopo aver attivato e configurato un Route 53 Resolver, puoi anche aggiungere endpoint sia in entrata sia in uscita per risolvere le query DNS da e verso la tua rete on-premise.

Configurazione di endpoint in uscita per Resolver su Outpost

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona il segno di spunta accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Nella tabella Endpoint in uscita, seleziona Crea endpoint in uscita.
6. Nella pagina Crea servizio endpoint in uscita, inserisci i valori applicabili. Per ulteriori informazioni, consulta Valori da specificare durante la creazione o la modifica di endpoint in entrata su un Outpost.

7. Seleziona Crea endpoint.

Valori da specificare durante la creazione o la modifica degli endpoint in uscita su un AWS Outposts

Quando crei o modifichi un endpoint in entrata, devi specificare i seguenti valori:

ID Outpost

Se stai creando l'endpoint per un Resolver su un AWS Outposts VPC, questo è l'ID. AWS Outposts

Nome endpoint

Un nome descrittivo che ti consenta di trovare facilmente un endpoint in entrata nel pannello di controllo.

VPC nella regione region-name.

Tutte le query DNS in entrata dalla rete passano per questo VPC in direzione di Resolver.

Gruppo di sicurezza per questo endpoint

L'ID di uno o più gruppi di sicurezza che si desidera utilizzare per controllare l'accesso a questo VPC. Il gruppo di sicurezza specificato deve includere una o più regole in entrata. Le regole in entrata devono autorizzare l'accesso TCP e UDP sulla porta 53. Non puoi modificare questo valore dopo avere creato l'endpoint.

Per ulteriori informazioni, consulta Gruppi di sicurezza per il VPC nella Guida per l'utente di Amazon VPC.

Indcirizzi IP

Gli indirizzi IP a cui vuoi che i resolver DNS sulla rete inoltrino le query DNS. Richiediamo di specificare un minimo di due indirizzi IP per la ridondanza. Tieni presente quanto segue:

Indirizzi IP e interfacce di rete elastiche di Amazon VPC

Per ogni combinazione di zona di disponibilità, sottorete e indirizzo IP specificata, Resolver crea un'interfaccia di rete elastica di Amazon VPC. Per quanto riguarda il numero massimo di query DNS al secondo per ogni indirizzo IP in un endpoint, consulta Quote relative a Route 53 Resolver. Per informazioni sui prezzi per ogni interfaccia di rete elastica, consulta "Amazon Route 53" nella Pagina dei prezzi di Amazon Route 53.

> **Note**
>
> L'endpoint del risolutore ha un indirizzo IP privato. Questi indirizzi IP non cambieranno nel corso della vita di un endpoint.

Per ogni indirizzo IP, specifica i seguenti valori. Ogni indirizzo IP deve trovarsi in una zona di disponibilità del VPC specificato in VPC in the region-name Region (VPC nella regione region-name).

Zona di disponibilità

La zona di disponibilità nella quale desideri che le query DNS passino in direzione del VPC. La zona di disponibilità specificata deve essere configurata con una sottorete.

Sottorete

La sottorete contenente l'indirizzo IP a cui si desidera inoltrare le query DNS. La sottorete deve avere a disposizione un indirizzo IP.

Specificare la sottorete per un indirizzo. IPv4 IPv6 non è supportata.

Indirizzo IP

L'indirizzo IP al quale desideri inoltrare le query DNS.

Scegli se vuoi che sia Resolver a scegliere un indirizzo IP per tuo conto tra gli indirizzi IP disponibili nella sottorete specificata o se vuoi specificare personalmente l'indirizzo IP.

Se scegli di specificare tu stesso l'indirizzo IP, inserisci un IPv4 indirizzo. IPv6 non è supportato.

Tag

Specifica una o più chiavi e i relativi valori. Ad esempio, è possibile specificare Cost center (Centro di costo) per Key (Chiave) e specificare 456 per Value (Valore).

Questi sono i tag che AWS Billing and Cost Management consentono di organizzare la AWS fattura; è possibile utilizzare anche i tag per altri scopi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consulta Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Creazione di regole di inoltro per endpoint in uscita

Puoi anche creare regole di inoltro per endpoint in uscita. Per ulteriori informazioni, consulta Per creare regole di inoltro e associarle a una o più regole VPCs

Gestione di Resolver su Outpost

Per gestire Resolver su Outpost, esegui la procedura applicabile.

Argomenti

Come modificare Resolver su Outpost

Per modificare un Resolver su Outpost, attieniti alla procedura seguente.

Modifica di un Resolver su Outpost

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona il segno di spunta accanto al Resolver in stato operativo e seleziona Modifica.
5. Puoi modificare le seguenti informazioni:
    - il nome del Resolver
    - il tipo di istanza
    - Il numero di istanze
6. Dopo aver terminato la modifica, seleziona Salva modifiche.

Visualizzazione dello stato di Resolver su Outpost

Per visualizzare lo stato di un Resolver su Outpost, attieniti alla procedura seguente.

Per visualizzare lo stato di un endpoint in entrata

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona il segno di spunta accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. La colonna Stato nella pagina Resolver su Outpost contiene uno dei seguenti valori:

   Creazione

   È in corso la creazione del Resolver su Outpost.

   Operational

   Il Resolver su Outpost è configurato correttamente.

   Aggiornamento in corso

   Il Resolver su Outpost sta aggiornando i tipi di istanze.

   Action needed

   Questo Resolver non è integro e non può essere ripristinato automaticamente. Per risolvere il problema, ti consigliamo di assicurarti che l'istanza sia in AWS Outposts grado di supportare Resolver su Outpost.

   Eliminazione in corso

   È in corso l'eliminazione del Resolver su Outpost.

   Creazione non riuscita

   La creazione di Resolver su Outpost non è andata a buon fine.

   Eliminazione non riuscita

   L'eliminazione di Resolver su Outpost non è andata a buon fine. Per risolvere il problema, ritenta tra qualche minuto.

Come eliminare Resolver su Outpost

> **Note**
>
> Prima di poter eliminare un Resolver su Outpost devi prima eliminare tutti gli endpoint ad esso associati.

Per eliminare un Resolver su Outpost, attieniti alla procedura seguente.

Eliminazione di un Resolver su Outpost

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Elimina.
5. Nella finestra di dialogo Elimina Resolver, digita **`delete`** nella casella di testo, quindi seleziona Elimina.

Come gestire endpoint in entrata su Resolver su Outpost

Per gestire gli endpoint in entrata su Resolver su Outpost, esegui la procedura applicabile.

Argomenti

- Visualizzazione e modifica degli endpoint in entrata
- Visualizzazione dello stato degli endpoint in entrata
- Eliminazione degli endpoint in entrata

Visualizzazione e modifica degli endpoint in entrata

Per visualizzare e modificare le impostazioni di un endpoint in entrata, procedi nel seguente modo.

Per visualizzare e modificare le impostazioni di un endpoint in entrata.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Dall'elenco degli Endpoint in entrata seleziona l'opzione per l'endpoint di cui desideri visualizzare o modificare le impostazioni.
6. Scegliere View details (Visualizza dettagli) o Edit (Modifica).

   Per informazioni sui valori per gli endpoint in entrata, consulta Valori da specificare durante la creazione o la modifica di endpoint in entrata su un Outpost.
7. Se si sceglie Edit (Modifica), immettere i valori applicabili e selezionare Save (Salva).

Visualizzazione dello stato degli endpoint in entrata

Per visualizzare lo stato di un endpoint in entrata, eseguire la procedura seguente.

Per visualizzare lo stato di un endpoint in entrata

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. La colonna Stato dell'elenco degli Endpoint in entrata contiene uno dei seguenti valori:

   Creazione

   Resolver crea e configura una o più interfacce di rete di Amazon VPC per questo endpoint.

Operational

Le interfacce di rete di Amazon VPC per questo endpoint sono configurate correttamente e in grado di inoltrare il traffico in entrata e in uscita delle query DNS tra la rete e Resolver.

Aggiornamento in corso

Il resolver associa o annulla l'associazione di una o più interfacce di rete a questo endpoint.

Auto recovering

Resolver prova a ripristinare una o più interfacce di rete associate a questo endpoint. Durante il processo di ripristino, l'endpoint funziona con capacità limitata a causa del limite del numero di query DNS per indirizzo IP (per interfaccia di rete). Per il limite corrente, consulta Quote relative a Route 53 Resolver.

Action needed

Questo endpoint non è integro e Resolver non è in grado di ripristinarlo automaticamente. Per risolvere il problema, si consiglia di verificare ciascun indirizzo IP associato all'endpoint. Per ogni indirizzo IP non disponibile, aggiungere un altro indirizzo IP e quindi eliminare l'indirizzo IP non disponibile. Un endpoint deve sempre includere almeno due indirizzi IP. Un stato di Action needed (Operazione necessaria) può avere una serie di cause. Di seguito sono illustrate due cause comuni:

- Una o più interfacce di rete associate con l'endpoint sono state eliminate tramite Amazon VPC.
- Non è stato possibile creare l'interfaccia di rete per motivi al di fuori del controllo di Resolver.

Eliminazione in corso

Il resolver sta eliminando questo endpoint e le interfacce di rete associate.

Eliminazione degli endpoint in entrata

Per eliminare un endpoint in entrata, procedi nel seguente modo.

> **Important**
>
> Se elimini un endpoint in entrata, le query DNS dalla rete non vengono più inoltrare a Resolver nel VPC specificato nell'endpoint.

Per eliminare un endpoint in entrata

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Scegli la casella di controllo accanto all'endpoint che desideri eliminare.
6. Scegli Elimina.
7. Per confermare che si desidera eliminare l'endpoint, immettere il nome dell'endpoint e scegliere Submit (Invia).

Come gestire endpoint in uscita su Resolver su Outpost

Per gestire gli endpoint in uscita su Resolver su Outpost, esegui la procedura applicabile.

Argomenti

Visualizzazione e modifica degli endpoint in uscita

Per visualizzare e modificare le impostazioni di un endpoint in uscita, procedi nel seguente modo.

Per visualizzare e modificare le impostazioni di un endpoint in uscita.

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Dall'elenco degli Endpoint in uscita seleziona l'opzione per l'endpoint di cui desideri visualizzare o modificare le impostazioni.
6. Scegliere View details (Visualizza dettagli) o Edit (Modifica).

   Per informazioni sui valori per gli endpoint in uscita, consulta Valori da specificare durante la creazione o la modifica degli endpoint in uscita su un AWS Outposts.
7. Se si sceglie Edit (Modifica), immettere i valori applicabili, quindi selezionare Save (Salva).

Visualizzazione dello stato degli endpoint in uscita

Per visualizzare lo stato di un endpoint in uscita, eseguire la procedura seguente.

Per visualizzare lo stato di un endpoint in uscita

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Nella barra di navigazione, scegli la regione in cui ti AWS Outposts trovi.
4. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
5. Nell'elenco Endpoint in uscita la colonna Stato contiene uno dei seguenti valori:

   Creazione

   Resolver crea e configura una o più interfacce di rete di Amazon VPC per questo endpoint.

   Operational

   Le interfacce di rete di Amazon VPC per questo endpoint sono configurate correttamente e in grado di inoltrare il traffico in entrata e in uscita delle query DNS tra la rete e Resolver.

   Aggiornamento in corso

   Il resolver associa o annulla l'associazione di una o più interfacce di rete a questo endpoint.

Auto recovering

Resolver prova a ripristinare una o più interfacce di rete associate a questo endpoint. Durante il processo di ripristino, l'endpoint funziona con capacità limitata a causa del limite del numero di query DNS per indirizzo IP (per interfaccia di rete). Per il limite corrente, consulta Quote relative a Route 53 Resolver.

Action needed

Questo endpoint non è integro e Resolver non è in grado di ripristinarlo automaticamente. Per risolvere il problema, si consiglia di verificare ciascun indirizzo IP associato all'endpoint. Per ogni indirizzo IP non disponibile, aggiungere un altro indirizzo IP e quindi eliminare l'indirizzo IP non disponibile. (Un endpoint deve sempre includere almeno due indirizzi IP). Un stato di Action needed (Operazione necessaria) può avere una serie di cause. Di seguito sono illustrate due cause comuni:

- Una o più interfacce di rete associate con l'endpoint sono state eliminate tramite Amazon VPC.
- Non è stato possibile creare l'interfaccia di rete per motivi al di fuori del controllo di Resolver.

Eliminazione in corso

Il resolver sta eliminando questo endpoint e le interfacce di rete associate.

Eliminazione degli endpoint in uscita

Prima di poter eliminare un endpoint, devi prima eliminare tutte le regole associate a un VPC.

Per eliminare un endpoint in uscita, procedi nel seguente modo.

> **Important**
>
> Se elimini un endpoint in uscita, Resolver smette di inoltrare query DNS dal tuo VPC alla rete per le regole che specificano l'endpoint in uscita eliminato.

Per eliminare un endpoint in uscita

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

2. Nel pannello di navigazione a sinistra espandi Resolver e vai su Outposts.
3. Seleziona la casella di controllo accanto al Resolver in stato operativo e seleziona Visualizza dettagli.
4. Dall'elenco degli Endpoint in uscita seleziona l'opzione per l'endpoint che desideri eliminare.
5. Scegli Elimina.
6. Per confermare che si desidera eliminare l'endpoint, immettere il nome dell'endpoint, quindi scegliere Submit (Invia).

Creazione di Amazon Route 53 e Amazon Route 53 Resolver risorse con AWS CloudFormation

Amazon Route 53 e Amazon Route 53 Resolver sono integrati con AWS CloudFormation un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri e fornisce AWS CloudFormation e configura tali risorse per te.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse Route 53 e Route 53 Resolver in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi distribuisci le stesse risorse più e più volte in più Account AWS regioni.

Route 53, Route 53 Resolver e modelli AWS CloudFormation

Per eseguire l'assegnazione e la configurazione delle risorse per Route 53 e i servizi correlati, devi comprendere i modelli AWS CloudFormation. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri inserire nei tuoi AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

Route 53 supporta la creazione dei seguenti tipi di risorse in: AWS CloudFormation

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse, consulta Riferimento ai tipi di risorse Amazon Route 53 nella Guida per l'utente di AWS CloudFormation .

Route 53 Resolver supporta la creazione dei seguenti tipi di risorse in: AWS CloudFormation

- `AWS::Route53Resolver::FirewallDomainList`

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallRuleGroupAssociation`
- `AWS::Route53Resolver::ResolverDNSSECConfig`
- `AWS::Route53Resolver::ResolverEndpoint`
- `AWS::Route53Resolver::ResolverQueryLoggingConfig`
- `AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`
- `AWS::Route53Resolver::ResolverRule`
- `AWS::Route53Resolver::ResolverRuleAssociation`

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse di Route 53 Resolver, consulta Riferimento ai tipi di risorse Amazon Route 53 Resolver nella Guida per l'utente di AWS CloudFormation .

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Documentazione di riferimento API
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Esempi di codice per l'utilizzo di Route 53 AWS SDKs

I seguenti esempi di codice mostrano come utilizzare Route 53 con un kit di sviluppo AWS software (SDK).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Utilizzare ListPrices con un SDK AWS
- Utilizzo RegisterDomain con un AWS SDK o una CLI
- Utilizzo ViewBilling con un AWS SDK o una CLI

Esempi di codice per l'utilizzo di Route 53 AWS SDKs

I seguenti esempi di codice mostrano come utilizzare Route 53 con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice

- Esempi di base per l'utilizzo di Route 53 AWS SDKs
  - Azioni per l'utilizzo di Route 53 AWS SDKs
    - Utilizzare ChangeResourceRecordSets con una CLI
    - Utilizzare CreateHostedZone con una CLI
    - Utilizzare DeleteHostedZone con una CLI
    - Utilizzare GetHostedZone con una CLI
    - Utilizzo ListHostedZones con un AWS SDK o una CLI
    - Utilizzare ListHostedZonesByName con una CLI
    - Utilizzare ListQueryLoggingConfigs con una CLI

Esempi di base per l'utilizzo di Route 53 AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Amazon Route 53 con AWS SDKs.

Esempi

- Azioni per l'utilizzo di Route 53 AWS SDKs

- Utilizzare ChangeResourceRecordSets con una CLI
- Utilizzare CreateHostedZone con una CLI
- Utilizzare DeleteHostedZone con una CLI
- Utilizzare GetHostedZone con una CLI
- Utilizzo ListHostedZones con un AWS SDK o una CLI
- Utilizzare ListHostedZonesByName con una CLI
- Utilizzare ListQueryLoggingConfigs con una CLI

Azioni per l'utilizzo di Route 53 AWS SDKs

I seguenti esempi di codice mostrano come eseguire singole azioni di Route 53 con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento delle API Amazon Route 53.

Esempi

- Utilizzare ChangeResourceRecordSets con una CLI
- Utilizzare CreateHostedZone con una CLI
- Utilizzare DeleteHostedZone con una CLI
- Utilizzare GetHostedZone con una CLI
- Utilizzo ListHostedZones con un AWS SDK o una CLI
- Utilizzare ListHostedZonesByName con una CLI
- Utilizzare ListQueryLoggingConfigs con una CLI

Utilizzare **`ChangeResourceRecordSets`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ChangeResourceRecordSets`.

CLI

AWS CLI

Per creare, aggiornare o eliminare un set di record di risorse

Il `change-resource-record-sets` comando seguente crea un set di record di risorse utilizzando la `hosted-zone-id` `Z1R8UBAEXAMPLE` configurazione in formato JSON contenuta nel file: `C:\awscli\route53\change-resource-record-sets.json`

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Per ulteriori informazioni, consulta POST ChangeResourceRecordSets nel riferimento dell'API Amazon Route 53.

La configurazione nel file JSON dipende dal tipo di set di record di risorse che desideri creare:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

Sintassi di base:

```
{
  "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"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Sintassi ponderata:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintassi degli alias:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
```

```
    {...}
  ]
}
```

Sintassi degli alias ponderati:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintassi della latenza:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintassi dell'alias di latenza:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintassi di failover:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

Sintassi degli alias di failover:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
```

```
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

- Per i dettagli sull'API, vedere ChangeResourceRecordSetsin AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: questo esempio crea un record A per www.example.com e modifica il record A per test.example.com da 192.0.2.3 a 192.0.2.1. Nota che i valori per le modifiche ai record di tipo TXT devono essere racchiusi tra virgolette doppie. Per ulteriori dettagli, consulta la documentazione di Amazon Route 53. Puoi utilizzare il Get-R53Change cmdlet per effettuare un sondaggio per determinare quando le modifiche sono state completate.

```
$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
```

Esempio 2: questo esempio mostra come creare set di record di risorse alias. 'Z222222222' è l'ID della zona ospitata di Amazon Route 53 in cui stai creando il set di record di risorse alias. 'example.com' è l'apice della zona per cui desideri creare un alias e 'www.example.com' è un sottodominio per il quale desideri creare anche un alias. 'Z11111' è un esempio di ID di zona ospitata per il sistema di bilanciamento del carico e 'example-load-balancer-11.us-east-1.elb.amazonaws.com' è un esempio di nome di dominio del load balancer con cui Amazon Route 53 risponde alle domande relative a example.com e www.example.com. Per ulteriori dettagli, consulta la documentazione di Amazon Route 53. Puoi utilizzare il Get-R53Change cmdlet per effettuare un sondaggio per determinare quando le modifiche sono state completate.

```
$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
```

Esempio 3: questo esempio crea due record A per www.example.com. Un quarto delle volte (1/ (1+3)), Amazon Route 53 risponde alle domande relative a www.example.com con i due valori del primo set di record di risorse (192.0.2.9 e 192.0.2.10). Tre quarti delle volte (3/ (1+3)) Amazon Route 53 risponde alle query relative a www.example.com con i due valori del secondo set di record di risorse (192.0.2.11 e 192.0.2.12). Per ulteriori dettagli, consulta la documentazione di Amazon Route 53. Puoi utilizzare il Get-R53Change cmdlet per effettuare un sondaggio per determinare quando le modifiche sono state completate.

```
$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
```

Esempio 4: Questo esempio mostra come creare set di record di risorse alias ponderati presupponendo che example.com sia il dominio per il quale si desidera creare set di record di risorse alias ponderati. SetIdentifier differenzia i due set di record di risorse alias ponderati l'uno dall'altro. Questo elemento è obbligatorio perché gli elementi Name e Type hanno gli stessi valori per entrambi i set di record di risorse. Z11111 e Z33333 sono esempi di zona ospitata IDs per il sistema di bilanciamento del carico ELB specificato dal valore di. DNSName example-load-balancer-2222222222.us-east-1.elb.amazonaws.com e example-load-balancer -4444444444.us-east-1.elb.amazonaws.com sono esempi di domini Elastic Load Balancing da cui Amazon Route 53 risponde alle domande per example.com. Per ulteriori dettagli, consulta la documentazione di Amazon Route 53. Puoi utilizzare il Get-R53Change cmdlet per effettuare un sondaggio per determinare quando le modifiche sono state completate.

```
$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
```

Esempio 5: Questo esempio crea due set di record di risorse con alias di latenza, uno per un sistema di bilanciamento del carico ELB nella regione Stati Uniti occidentali (Oregon) (us-west-2) e un altro per un sistema di bilanciamento del carico nella regione Asia Pacifico (Singapore) (ap-southeast-1). Per ulteriori dettagli, consulta la documentazione di Amazon Route 53. Puoi utilizzare il Get-R53Change cmdlet per effettuare un sondaggio per determinare quando le modifiche sono state completate.

```
$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
```

- Per i dettagli sull'API, vedere ChangeResourceRecordSetsin AWS Strumenti per PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`CreateHostedZone`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CreateHostedZone`.

CLI

AWS CLI

Per creare una zona ospitata

Il `create-hosted-zone` comando seguente aggiunge una zona ospitata denominata `example.com` utilizzando il riferimento del chiamante. `2014-04-01-18:47` Il commento opzionale include uno spazio, quindi deve essere racchiuso tra virgolette:

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Per ulteriori informazioni, consulta Working with Hosted Zones nella Amazon Route 53 Developer Guide.

- Per i dettagli sull'API, consulta CreateHostedZone AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: crea una nuova zona ospitata denominata 'example.com', associata a un set di deleghe riutilizzabile. Si noti che è necessario fornire un valore per il CallerReference parametro in modo che le richieste in questione debbano essere ritentate, se necessario, senza il rischio di eseguire l'operazione due volte. Poiché la zona ospitata viene creata in un VPC, è automaticamente privata e non è necessario impostare il parametro - HostedZoneConfig _PrivateZone .

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- Per i dettagli sull'API, vedere CreateHostedZonein AWS Strumenti per PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`DeleteHostedZone`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `DeleteHostedZone`.

CLI

AWS CLI

Per eliminare una zona ospitata

Il `delete-hosted-zone` comando seguente elimina la zona ospitata con un `id` di`Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Per i dettagli sull'API, vedere DeleteHostedZonein AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: elimina la zona ospitata con l'ID specificato. Ti verrà richiesta una conferma prima di procedere con il comando, a meno che tu non aggiunga il parametro -Force switch.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Per i dettagli sull'API, vedere DeleteHostedZonein AWS Strumenti per PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`GetHostedZone`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetHostedZone`.

CLI

AWS CLI

Per ottenere informazioni su una zona ospitata

Il `get-hosted-zone` comando seguente ottiene informazioni sulla zona ospitata con un `id` di`Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Per i dettagli sull'API, vedere GetHostedZonein AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce i dettagli della zona ospitata con ID PJN98 FT9 Z1D633.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Per i dettagli sull'API, vedere GetHostedZonein Cmdlet Reference.AWS Strumenti per PowerShell

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListHostedZones`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListHostedZones`.

CLI

AWS CLI

Per elencare le zone ospitate associate all'account corrente AWS

Il `list-hosted-zones` comando seguente elenca le informazioni di riepilogo sulle prime 100 zone ospitate associate all' AWS account corrente. :

```
aws route53 list-hosted-zones
```

Se disponi di oltre 100 zone ospitate o se desideri elencarle in gruppi più piccoli di 100, includi il parametro `--max-items`. Ad esempio, per elencare le zone ospitate una alla volta, utilizza il comando seguente:

```
aws route53 list-hosted-zones --max-items 1
```

Per visualizzare le informazioni sulla zona ospitata successiva, prendi il valore di `NextToken` dalla risposta al comando precedente e includilo nel parametro `--starting-token`, ad esempio:

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Per i dettagli sull'API, consulta ListHostedZones AWS CLICommand Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: emette tutte le zone ospitate pubbliche e private.

```
Get-R53HostedZoneList
```

Esempio 2: restituisce tutte le zone ospitate associate al set di deleghe riutilizzabile con ID X2CISAMPLE NZ8

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Per i dettagli sull'API, vedere in Cmdlet Reference. ListHostedZonesAWS Strumenti per PowerShell

Rust

SDK per Rust

> **Note**
>
> C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
 aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!("  ID :   {}", zone_id);
        println!("  Name : {}", zone_name);
        println!();
    }

    Ok(())
}
```

- Per i dettagli sulle API, consulta la ListHostedZonesguida di riferimento all'API AWS SDK for Rust.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`ListHostedZonesByName`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListHostedZonesByName`.

CLI

AWS CLI

Il comando seguente elenca fino a 100 zone ospitate ordinate per nome di dominio:

```
aws route53 list-hosted-zones-by-name
```

Output:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-2",
          "Config": {
              "Comment": "test2",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z119WBBTVP5WFX",
          "Name": "2.example.com."
      },
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
          "Name": "www.example.com."
      }
  ],
  "IsTruncated": false,
  "MaxItems": "100"
```

```
}
```

Il comando seguente elenca le zone ospitate ordinate per nome, a partire da`www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Output:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "mwunderl20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
          "Name": "www.example.com."
      }
  ],
  "DNSName": "www.example.com",
  "IsTruncated": false,
  "MaxItems": "100"
}
```

- Per i dettagli sull'API, vedere ListHostedZonesByNamein AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell

Esempio 1: restituisce tutte le zone ospitate pubbliche e private in ordine ASCII per nome di dominio.

```
Get-R53HostedZonesByName
```

Esempio 2: restituisce le zone ospitate pubbliche e private, in ordine ASCII per nome di dominio, a partire dal nome DNS specificato.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- Per i dettagli sull'API, vedere ListHostedZonesByNamein AWS Strumenti per PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`ListQueryLoggingConfigs`** con una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListQueryLoggingConfigs`.

CLI

AWS CLI

Per elencare le configurazioni di registrazione delle query

L'`list-query-logging-configs`esempio seguente elenca le informazioni sulle prime 100 configurazioni di registrazione delle query nell' AWS account, per la zona ospitata. `Z1OX3WQEXAMPLE`

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

Output:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

Per ulteriori informazioni, consulta la sezione Registrazione delle query DNS nella Amazon Route 53 Developer Guide.

- Per i dettagli sull'API, consulta Command ListQueryLoggingConfigsReference AWS CLI .

PowerShell

Strumenti per PowerShell

Esempio 1: Questo esempio restituisce tutte le configurazioni per la registrazione delle query DNS associate alla versione corrente. Account AWS

```
Get-R53QueryLoggingConfigList
```

Output:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- Per i dettagli sull'API, vedere ListQueryLoggingConfigsin AWS Strumenti per PowerShell Cmdlet Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Esempi di codice per la registrazione di domini Route 53 utilizzando AWS SDKs

I seguenti esempi di codice mostrano come utilizzare la registrazione del dominio Route 53 con un kit di sviluppo AWS software (SDK).

Le nozioni di base sono esempi di codice che mostrano come eseguire le operazioni essenziali all'interno di un servizio.

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Nozioni di base

Registrazione domini Hello Route 53

Gli esempi di codice seguenti mostrano come iniziare a usare la registrazione di domini Route 53.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();
```

```
        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- Per i dettagli sull'API, consulta la ListPricessezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
```

```
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
 String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
```

```
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
 route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
 pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
 + pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
 pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Per i dettagli sull'API, consulta la ListPricessezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.

 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
```

```
        }

    Route53DomainsClient { 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}")
            }
    }
}
```

- Per i dettagli sull'API, ListPricesconsulta AWS SDK for Kotlin API reference.

Esempi di codice

- Esempi di base per la registrazione di domini Route 53 utilizzando AWS SDKs
  - Registrazione domini Hello Route 53
  - Scopri le nozioni di base sulla registrazione dei domini Route 53 con un SDK AWS
  - Azioni per la registrazione del dominio Route 53 utilizzando AWS SDKs
    - Utilizzo CheckDomainAvailability con un AWS SDK o una CLI
    - Utilizzo CheckDomainTransferability con un AWS SDK o una CLI
    - Utilizzo GetDomainDetail con un AWS SDK o una CLI
    - Utilizzo GetDomainSuggestions con un AWS SDK o una CLI
    - Utilizzo GetOperationDetail con un AWS SDK o una CLI
    - Utilizzo ListDomains con un AWS SDK o una CLI
    - Utilizzo ListOperations con un AWS SDK o una CLI
    - Utilizzare ListPrices con un SDK AWS
    - Utilizzo RegisterDomain con un AWS SDK o una CLI
    - Utilizzo ViewBilling con un AWS SDK o una CLI

Esempi di base per la registrazione di domini Route 53 utilizzando AWS SDKs

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di Amazon Route 53 domain registration with. AWS SDKs

Esempi

- Registrazione domini Hello Route 53
- Scopri le nozioni di base sulla registrazione dei domini Route 53 con un SDK AWS
- Azioni per la registrazione del dominio Route 53 utilizzando AWS SDKs
  - Utilizzo CheckDomainAvailability con un AWS SDK o una CLI
  - Utilizzo CheckDomainTransferability con un AWS SDK o una CLI
  - Utilizzo GetDomainDetail con un AWS SDK o una CLI
  - Utilizzo GetDomainSuggestions con un AWS SDK o una CLI
  - Utilizzo GetOperationDetail con un AWS SDK o una CLI
  - Utilizzo ListDomains con un AWS SDK o una CLI
  - Utilizzo ListOperations con un AWS SDK o una CLI
  - Utilizzare ListPrices con un SDK AWS
  - Utilizzo RegisterDomain con un AWS SDK o una CLI
  - Utilizzo ViewBilling con un AWS SDK o una CLI

Registrazione domini Hello Route 53

Gli esempi di codice seguenti mostrano come iniziare a usare la registrazione di domini Route 53.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- Per i dettagli sull'API, consulta la ListPricessezione AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
```

```
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
+ pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
" + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
pr.changeOwnershipPrice().price() + " "
```

```
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Per i dettagli sull'API, consulta la ListPricessezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.

 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
```

```
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient { 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}")
            }
    }
}
```

- Per i dettagli sull'API, ListPricesconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Scopri le nozioni di base sulla registrazione dei domini Route 53 con un SDK AWS

Gli esempi di codice seguenti mostrano come:

- Elenca i domini correnti ed elenca le operazioni dell'anno scorso.
- Visualizza la fatturazione dell'anno scorso e visualizza i prezzi per i tipi di dominio.
- Ricevi suggerimenti sui domini.
- Verifica la disponibilità e la trasferibilità dei domini.
- Facoltativamente, richiedi la registrazione di un dominio.
- Ottieni informazioni dettagliate di un'operazione.
- Facoltativamente, ottieni informazioni dettagliate di un dominio.

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

Esegui uno scenario interattivo al prompt dei comandi.

```
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;
    }
}
```

Metodi wrapper utilizzati dallo scenario per le operazioni di registrazione di domini Route 53.

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
 ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }


    /// <summary>
```

```
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }


    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Availability.Value;
    }


    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
```

```
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }


    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }


    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
```

```
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
 {operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }


    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
```

```
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
{domainName}");
            return null;
        }
    }


    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }
```

```
    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }


    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }
```

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
 {result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento API di AWS SDK for .NET .
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices

- RegisterDomain
- ViewBilling

Java

SDK per Java 2.x

> **Note**
>
> C'è dell'altro GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
 *
 * This Java code example performs the following operations:
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
 * 4. View prices for domain types.
 * 5. Get domain suggestions.
 * 6. Check domain availability.
 * 7. Check domain transferability.
 * 8. Request a domain registration.
 * 9. Get operation details.
```

```
 * 10. Optionally, get domain details.
 */

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <domainType> <phoneNumber> <email> <domainSuggestion>
 <firstName> <lastName> <city>

                Where:
                    domainType - The domain type (for example, com).\s
                    phoneNumber - The phone number to use (for example,
 +91.9966564xxx)      email - The email address to use.      domainSuggestion -
 The domain suggestion (for example, findmy.accountants).\s
                    firstName - The first name to use to register a domain.\s
                    lastName -  The last name to use to register a domain.\s
                    city - the city to use to register a domain.\s
                    """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
```

```
        System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. List current domains.");
        listDomains(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. List operations in the past year.");
        listOperations(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. View billing for the account in the past year.");
        listBillingRecords(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. View prices for domain types.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Get domain suggestions.");
        listDomainSuggestions(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
domainSuggestion, phoneNumber, email, firstName,
                lastName, city);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain 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);
        }
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento API di AWS SDK for Java 2.x .
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK per Kotlin

> **Note**
>
> C'è dell'altro GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.
```

```
For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
 */

val DASHES: String = String(CharArray(80)).replace("\u0000", "-")

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
 <lastName> <city>
        Where:
           domainType - The domain type (for example, com).
           phoneNumber - The phone number to use (for example, +1.2065550100)

           email - The email address to use.
           domainSuggestion - The domain suggestion (for example,
 findmy.example).
           firstName - The first name to use to register a domain.
           lastName -  The last name to use to register a domain.
           city - The city to use to register a domain.
    """

    if (args.size != 7) {
        println(usage)
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
```

```
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
    listOperations()
    println(DASHES)

    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("7. Check domain transferability.")
    checkDomainTransferability(domainSuggestion)
    println(DASHES)
```

```
    println(DASHES)
    println("8. Request a domain registration.")
    val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
 firstName, lastName, city)
    println(DASHES)

    println(DASHES)
    println("9. Get operation details.")
    getOperationalDetail(opId)
    println(DASHES)

    println(DASHES)
    println("10. Get domain details.")
    println("Note: You must have a registered domain to get details.")
    println("Otherwise an exception is thrown that states ")
    println("Domain 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}")
            }
    }
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Kotlin.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consultaUtilizzo di Route 53 con un SDK AWS. Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Azioni per la registrazione del dominio Route 53 utilizzando AWS SDKs

I seguenti esempi di codice mostrano come eseguire azioni di registrazione di singoli domini Route 53 con AWS SDKs. Ogni esempio include un collegamento a GitHub, dove sono disponibili le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta la Documentazione di riferimento API di Amazon Route 53 domain registration.

Esempi

- Utilizzo CheckDomainAvailability con un AWS SDK o una CLI
- Utilizzo CheckDomainTransferability con un AWS SDK o una CLI
- Utilizzo GetDomainDetail con un AWS SDK o una CLI
- Utilizzo GetDomainSuggestions con un AWS SDK o una CLI
- Utilizzo GetOperationDetail con un AWS SDK o una CLI
- Utilizzo ListDomains con un AWS SDK o una CLI
- Utilizzo ListOperations con un AWS SDK o una CLI

- Utilizzare ListPrices con un SDK AWS
- Utilizzo RegisterDomain con un AWS SDK o una CLI
- Utilizzo ViewBilling con un AWS SDK o una CLI

Utilizzo **`CheckDomainAvailability`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CheckDomainAvailability`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- Per i dettagli sull'API, consulta la CheckDomainAvailabilitysezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per determinare se è possibile registrare un nome di dominio con Route 53

Il `check-domain-availability` comando seguente restituisce informazioni sulla disponibilità del nome `example.com` di dominio per la registrazione tramite Route 53.

Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

Output:

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53 supporta un gran numero di domini di primo livello (TLDs), come `.com` e`.jp`, ma non supportiamo tutti i domini disponibili. TLDs Se verifichi la disponibilità di un dominio e Route 53 non supporta il dominio di primo livello, `check-domain-availability` restituisce il seguente messaggio.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Per un elenco dei domini TLDs che puoi utilizzare per registrare un dominio con Route 53, consulta Domini che puoi registrare con Amazon Route 53 nella Amazon Route 53 Developer Guide. Per ulteriori informazioni sulla registrazione di domini con Amazon Route 53, consulta Registrazione di un nuovo dominio nella Amazon Route 53 Developer Guide.

- Per i dettagli sull'API, consulta Command CheckDomainAvailabilityReference AWS CLI .

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainAvailabilityResponse response = route53DomainsClient
                   .checkDomainAvailability(availabilityRequest);
           System.out.println(domainSuggestion + " is " +
response.availability().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, consulta la CheckDomainAvailabilitysezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
    }
}
```

- Per i dettagli sull'API, CheckDomainAvailabilityconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`CheckDomainTransferability`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `CheckDomainTransferability`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Transferability.Transferable.Value;
}
```

- Per i dettagli sull'API, consulta la CheckDomainTransferabilitysezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per determinare se un dominio può essere trasferito su Route 53

Il `check-domain-transferability` comando seguente restituisce informazioni sulla possibilità di trasferire il nome `example.com` di dominio su Route 53.

Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Output:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

Per ulteriori informazioni, consulta Trasferimento della registrazione di un dominio su Amazon Route 53 nella Amazon Route 53 Developer Guide.

- Per i dettagli sull'API, consulta CheckDomainTransferability AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
```

```
            System.out.println("Transferability: " +
 response.transferability().transferable().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Per i dettagli sull'API, consulta la CheckDomainTransferabilitysezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
    }
}
```

- Per i dettagli sull'API, CheckDomainTransferabilityconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetDomainDetail`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetDomainDetail`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
{result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
```

```
                        $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
```

- Per i dettagli sull'API, consulta la GetDomainDetailsezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per ottenere informazioni dettagliate su un dominio specifico

Il `get-domain-detail` comando seguente visualizza informazioni dettagliate sul dominio specificato.

Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

Output:

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
```

```
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
```

```
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon.com",
    "RegistrarUrl": "http://registrar.amazon.com",
    "AbuseContactEmail": "abuse@registrar.amazon.com",
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- Per i dettagli sull'API, consulta GetDomainDetail AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
```

```
                    .build();

            GetDomainDetailResponse response =
 route53DomainsClient.getDomainDetail(detailRequest);
            System.out.println("The contact first name is " +
 response.registrantContact().firstName());
            System.out.println("The contact last name is " +
 response.registrantContact().lastName());
            System.out.println("The contact org name is " +
 response.registrantContact().organizationName());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Per i dettagli sull'API, consulta la GetDomainDetailsezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
    }
}
```

- Per i dettagli sull'API, GetDomainDetailconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetDomainSuggestions`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetDomainSuggestions`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
```

```
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }
```

- Per i dettagli sull'API, consulta la GetDomainSuggestionssezione AWS SDK for .NET API Reference.

CLI

AWS CLI

Per ottenere un elenco dei nomi di dominio suggeriti

Il `get-domain-suggestions` comando seguente visualizza un elenco di nomi di dominio suggeriti in base al nome di dominio`example.com`. La risposta include solo i nomi di dominio disponibili. Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

Output:

```
{
```

```
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
       },
        {
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- Per i dettagli sull'API, consulta GetDomainSuggestions AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                   .domainName(domainSuggestion)
                   .suggestionCount(5)
                   .onlyAvailable(true)
                   .build();

           GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
           List<DomainSuggestion> suggestions = response.suggestionsList();
           for (DomainSuggestion suggestion : suggestions) {
               System.out.println("Suggestion Name: " +
suggestion.domainName());
               System.out.println("Availability: " + suggestion.availability());
               System.out.println(" ");
           }

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, consulta la GetDomainSuggestionssezione AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è di più su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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(" ")
        }
    }
}
```

- Per i dettagli sull'API, GetDomainSuggestionsconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`GetOperationDetail`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `GetOperationDetail`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
```

```
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }
```

- Per i dettagli sull'API, GetOperationDetailconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Per ottenere lo stato corrente di un'operazione

Alcune operazioni di registrazione del dominio funzionano in modo asincrono e restituiscono una risposta prima del termine. Queste operazioni restituiscono un ID operativo che è possibile utilizzare per ottenere lo stato corrente. Il `get-operation-detail` comando seguente restituisce lo stato dell'operazione specificata.

Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Output:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- Per i dettagli sull'API, consulta GetOperationDetail AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, GetOperationDetailconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
    }
}
```

- Per i dettagli sull'API, GetOperationDetailconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListDomains`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListDomains`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
```

```
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
        }
        return results;
    }
```

- Per i dettagli sull'API, ListDomainsconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Per elencare i domini registrati con l'account corrente AWS

Il `list-domains` comando seguente elenca informazioni di riepilogo sui domini registrati con l'account corrente AWS .

Questo comando viene eseguito solo nella `us-east-1` regione. Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains list-domains
    --region us-east-1
```

Output:

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
```

```
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- Per i dettagli sull'API, consulta [ListDomains AWS CLI](#)Command Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
+ content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
```

```
        }
    }
```

- Per i dettagli sull'API, ListDomainsconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
            }
    }
}
```

- Per i dettagli sull'API, ListDomainsconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ListOperations`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ListOperations`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   /// <summary>
   /// List operations for the account that are submitted after a specified
date.
   /// </summary>
   /// <returns>A collection of operation summary records.</returns>
   public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
   {
       var results = new List<OperationSummary>();
       var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
           new ListOperationsRequest()
           {
               SubmittedSince = submittedSince
           });

       // Get the entire list using the paginator.
       await foreach (var operations in paginateOperations.Operations)
       {
           results.Add(operations);
       }
       return results;
   }
```

- Per i dettagli sull'API, ListOperationsconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Per elencare lo stato delle operazioni che restituiscono un ID operativo

Alcune operazioni di registrazione del dominio vengono eseguite in modo asincrono e restituiscono una risposta prima del termine. Queste operazioni restituiscono un ID operativo che puoi utilizzare per ottenere lo stato corrente. Il `list-operations` comando seguente elenca informazioni di riepilogo, incluso lo stato, sulle operazioni correnti di registrazione del dominio.

Questo comando viene eseguito solo nella regione. `us-east-1` Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains list-operations
    --region us-east-1
```

Output:

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
```

```
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

L'output include tutte le operazioni che restituiscono un ID di operazione e che hai eseguito su tutti i domini che hai mai registrato utilizzando l'account corrente AWS . Se desideri visualizzare solo le operazioni inviate dopo una data specificata, puoi includere il `submitted-since` parametro e specificare una data in formato Unix e nel Coordinated Universal Time (UTC). Il comando seguente ottiene lo stato di tutte le operazioni inviate dopo le 12:00 UTC del 1° gennaio 2020.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- Per i dettagli sull'API, consulta AWS CLI Command ListOperationsReference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void listOperations(Route53DomainsClient route53DomainsClient)
{
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           localDateTime = localDateTime.minusYears(1);
           Instant myTime = localDateTime.toInstant(zoneOffset);

           ListOperationsRequest operationsRequest =
ListOperationsRequest.builder()
```

```
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
 route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
 content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Per i dettagli sull'API, ListOperationsconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
```

```
        }

    Route53DomainsClient { 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}")
            }
    }
}
```

- Per i dettagli sull'API, ListOperationsconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzare **`ListPrices`** con un SDK AWS

Gli esempi di codice seguenti mostrano come utilizzare `ListPrices`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

- Per i dettagli sull'API, ListPricesconsulta AWS SDK for .NET API Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
```

```
                    .forEach(content -> System.out.println(" Name: " +
content.name() +
                            " Registration: " +
content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
                            " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Per i dettagli sull'API, ListPricesconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
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}")
            }
    }
}
```

- Per i dettagli sull'API, ListPricesconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`RegisterDomain`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `RegisterDomain`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
```

```
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
 {domainName}");
            return null;
        }
    }
```

- Per i dettagli sull'API, RegisterDomainconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Per registrare un dominio

Il `register-domain` comando seguente registra un dominio, recuperando tutti i valori dei parametri da un file in formato JSON.

Questo comando viene eseguito solo nella regione. `us-east-1` Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

Contenuto di `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
}
```

Output:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Per confermare che l'operazione è riuscita, puoi eseguire. `get-operation-detail` Per ulteriori informazioni, consulta get-operation-detail.

Per maggiori informazioni, consulta Registrazione di un nuovo dominio nella Guida per gli sviluppatori Amazon Route 53.

Per informazioni su quali domini di primo livello (TLDs) richiedono valori `ExtraParams` e quali sono i valori validi, consulta ExtraParamil riferimento alle API di Amazon Route 53.

- Per i dettagli sull'API, consulta AWS CLI Command RegisterDomainReference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
           String domainSuggestion,
           String phoneNumber,
           String email,
           String firstName,
           String lastName,
           String city) {

       try {
           ContactDetail contactDetail = ContactDetail.builder()
                   .contactType(ContactType.COMPANY)
                   .state("LA")
                   .countryCode(CountryCode.IN)
                   .email(email)
                   .firstName(firstName)
                   .lastName(lastName)
                   .city(city)
                   .phoneNumber(phoneNumber)
                   .organizationName("My Org")
                   .addressLine1("My Address")
                   .zipCode("123 123")
                   .build();

           RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                   .adminContact(contactDetail)
                   .registrantContact(contactDetail)
                   .techContact(contactDetail)
                   .domainName(domainSuggestion)
                   .autoRenew(true)
                   .durationInYears(1)
                   .build();
```

```
            RegisterDomainResponse response =
 route53DomainsClient.registerDomain(domainRequest);
            System.out.println("Registration requested. Operation Id: " +
 response.operationId());
            return response.operationId();

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- Per i dettagli sull'API, RegisterDomainconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
```

```
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- Per i dettagli sull'API, RegisterDomainconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Utilizzo **`ViewBilling`** con un AWS SDK o una CLI

Gli esempi di codice seguenti mostrano come utilizzare `ViewBilling`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- Informazioni di base

.NET

AWS SDK for .NET

> **Note**
>
> C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }
```

- Per i dettagli sull'API, ViewBillingconsulta AWS SDK for .NET API Reference.

CLI

AWS CLI

Per ottenere informazioni di fatturazione per i costi di registrazione del dominio per l'account corrente AWS

Il `view-billing` comando seguente restituisce tutti i record di fatturazione relativi al dominio per l'account corrente per il periodo compreso tra il 1° gennaio 2018 (1514764800 nel fuso orario Unix) e la mezzanotte del 31 dicembre 2019 (1577836800 nel fuso orario Unix).

Questo comando viene eseguito solo nella regione. `us-east-1` Se la regione predefinita è impostata su`us-east-1`, è possibile omettere il `region` parametro.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

Output:

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
}
```

Per ulteriori informazioni, consulta la ViewBillingpagina di riferimento dell'API Amazon Route 53.

- Per i dettagli sull'API, consulta ViewBilling AWS CLICommand Reference.

Java

SDK per Java 2.x

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();

           ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
           listRes.stream()
                   .flatMap(r -> r.billingRecords().stream())
                   .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                           " Operation: " + content.operationAsString() +
                           " Price: " + content.price()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Per i dettagli sull'API, ViewBillingconsulta AWS SDK for Java 2.x API Reference.

Kotlin

SDK per Kotlin

> **Note**
>
> C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel Repository di esempi di codice AWS.

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient { 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}")
            }
    }
}
```

- Per i dettagli sull'API, ViewBillingconsulta AWS SDK for Kotlin API reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. Utilizzo di Route 53 con un SDK AWS Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Sicurezza in Amazon Route 53

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Route 53, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usa Route 53. I seguenti argomenti illustrano come configurare Route 53 per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Route 53.

Argomenti

Protezione dei dati in Route 53

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Route 53. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura

globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Route 53 o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Protezione dai registri di deleghe con strascichi in Route 53

Con Route 53, un cliente può creare una zona ospitata, ad esempio `example.com` per ospitare i propri record DNS. Ogni zona ospitata è dotata di un «set di delega», ovvero un set di quattro name

server che un cliente può utilizzare per configurare i record NS nel dominio principale. Questi record NS possono essere chiamati «record NS di delega» o «record di delega».

Affinché la zona ospitata `example.com` Route 53 diventi autorevole, il legittimo proprietario del `example.com` dominio deve configurare i record di delega nel dominio principale «.com» tramite il registrar di domini. Nei casi in cui un cliente perda l'accesso ai quattro name server configurati nel dominio principale, ad esempio perché la zona ospitata associata viene eliminata, ciò può creare un rischio sfruttabile da un utente malintenzionato. Si tratta del cosiddetto rischio di «dati di delega sospesi».

La Route 53 protegge dal rischio di perdita di dati di delega nel caso in cui una zona ospitata venga eliminata. Dopo l'eliminazione, se viene creata una nuova zona ospitata con lo stesso nome di dominio, Route 53 verificherà se i record di delega che puntano alla zona ospitata eliminata sono ancora presenti nel dominio principale. Se lo sono, Route 53 impedirà l'assegnazione di name server sovrapposti. Questo è lo scenario 1 negli esempi seguenti.

Tuttavia, vi sono altri rischi legati ai record di delega, dai quali Route 53 non è in grado di proteggersi, come illustrato negli scenari 2 e 3 negli esempi seguenti. Per proteggerti da questo insieme più ampio di rischi, assicurati che i record NS principali corrispondano al set di delega per la zona ospitata da Route 53. È possibile trovare il set di delega di una zona ospitata tramite la console Route 53 oppure AWS CLI. Per ulteriori informazioni, consulta Elencazione di record o get-hosted-zone.

Inoltre, l'abilitazione della firma DNSSEC per una zona ospitata sulla Route 53 può fungere da ulteriore livello di protezione oltre alle best practice sopra menzionate. Il DNSSEC verifica che le risposte DNS provengano dalla fonte autorevole, proteggendo efficacemente da questo rischio. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

Esempi

Negli esempi seguenti, supponiamo che tu abbia un dominio e il relativo dominio figlio. `example.com` `child.example.com` Spiegheremo come in vari scenari si possono creare record di delega sospesi, in che modo Route 53 protegge il dominio dagli abusi e come mitigare efficacemente i rischi associati ai record di delega sospesi.

Scenario 1:

<ns3><ns4>Si crea una zona ospitata `child.example.com` con quattro name server:<ns1>,<ns2>, e. La delega viene configurata correttamente nella zona ospitata`example.com`, creando record NS `child.example.com` di delega per quattro name server <ns1><ns2>,<ns3>, e<ns4>. Quando la zona `child.example.com` ospitata

viene eliminata senza rimuovere i record NS della delega`example.com`, Route 53 protegge `child.example.com` dal rischio che i record di delega non funzionino <ns1><ns2><ns3>, impedendo <ns4>che vengano assegnati a zone ospitate di nuova creazione con lo stesso nome di dominio.

Scenario 2:

Simile allo scenario 1, ma questa volta si eliminano la zona ospitata dai minori E i record NS di delega nella zona `example.com` ospitata. Tuttavia, si aggiungono nuovamente i record NS di delega <ns1><ns2><ns3>e <ns4>senza creare una zona ospitata da un figlio. Qui si <ns1><ns2><ns3><ns4>tratta di record di delega in sospeso, poiché Route 53 rimuove il blocco, che impediva l'<ns1><ns2><ns3><ns4>assegnazione, e ora consentirà alle zone ospitate appena create di utilizzare server di nomi al di sopra dei name server. Per mitigare il rischio <ns1><ns2><ns3>, rimuovete «e» <ns4>dai record di delega e aggiungeteli nuovamente solo dopo aver creato la zona ospitata dai bambini.

Scenario 3:

<ns4>In questo scenario, si crea un set di delega riutilizzabile Route 53 con name server<ns1>, <ns2><ns3>, e. Quindi, delegate il dominio `example.com` a questi name server nel dominio principale. `.com` Tuttavia, non hai ancora creato la zona ospitata per `example.com` il set di delega riutilizzabile. Ecco,, <ns1><ns2><ns3>, e <ns4>ci sono documenti di delega sospesi. <ns3><ns4>Per mitigare il rischio, crea la zona ospitata utilizzando il set di delega riutilizzabile con name server<ns1>,<ns2>, e.

Identity and Access Management in Amazon Route 53

Per eseguire qualsiasi operazione sulle risorse Amazon Route 53, come la registrazione di un dominio o l'aggiornamento di un record, AWS Identity and Access Management (IAM) è necessario autenticare che sei un utente approvato AWS . Se stai utilizzando la console Route 53, autentichi la tua identità fornendo il tuo nome utente e una password AWS .

Dopo aver autenticato la tua identità, IAM controlla il tuo accesso AWS verificando che tu disponga delle autorizzazioni per eseguire operazioni e accedere alle risorse. Se sei un amministratore account, puoi utilizzare IAM per controllare l'accesso di altri utenti alle risorse associate al tuo account.

Questo capitolo descrive come utilizzare IAM e Route 53 per proteggere le tue risorse.

Argomenti

- Autenticazione con identità
- Controllo accessi
- Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Route 53
- Utilizzo di policy basate su identità (policy IAM) per Amazon Route 53
- Utilizzo di ruoli collegati ai servizi per Amazon Route 53 Resolver
- AWS politiche gestite per Amazon Route 53
- Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi
- Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti

alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Controllo accessi

Per creare, aggiornare, eliminare o elencare le risorse di Amazon Route 53 hai bisogno delle autorizzazioni per eseguire l'operazione e l'autorizzazione per accedere alle risorse corrispondenti.

Nelle sezioni seguenti viene descritto come gestire le autorizzazioni per Route 53. Consigliamo di leggere prima la panoramica.

Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Route 53

Ogni AWS risorsa è di proprietà di un AWS account e le autorizzazioni per creare o accedere a una risorsa sono regolate da politiche di autorizzazione.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni sugli amministratori, consulta Best practice IAM nella Guida per l'utente di IAM.

Quando concedi le autorizzazioni, devi specificare gli utenti che le riceveranno e le risorse per cui le concedi, nonché le operazioni specifiche per cui ottengono le autorizzazioni.

Gli utenti necessitano dell'accesso programmatico se desiderano interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche a AWS CLI,, AWS SDKs o. AWS APIs	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, vedere Configurazione dell'uso AWS IAM Identity Center

Quale utente necessita dell'accesso programmatico?	Per	Come
		nella AWS CLI Guida per l'utente.AWS Command Line Interface • Per AWS SDKs gli strumenti e AWS APIs, consulta l'autenticazione di IAM Identity Center nella Guida di riferimento AWS SDKs and Tools.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche a AWS CLI, AWS SDKs, o. AWS APIs	Seguendo le istruzioni riportate in Utilizzo delle credenziali temporanee con le AWS risorse nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche a AWS CLI,, AWS SDKs o. AWS APIs	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli strumenti AWS SDKs e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli strumenti e agli AWS SDKs strumenti. • Per AWS APIs, consulta la sezione Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Argomenti

- ARNs per le risorse Amazon Route 53
- Informazioni sulla proprietà delle risorse
- Gestione dell'accesso alle risorse
- Definizione degli elementi delle policy: risorse, operazioni, effetti ed entità principali
- Specifica delle condizioni in una policy

ARNs per le risorse Amazon Route 53

Amazon Route 53 supporta diversi tipi di risorse per il DNS, il controllo dell'integrità e la registrazione dei domini. In una policy, puoi concedere o negare l'accesso alle seguenti risorse utilizzando * per l'ARN:

- Controlli dell'integrità
- Zona ospitata
- Set di deleghe riutilizzabili
- Status di un set di record di risorse modifica batch (API)
- Policy di traffico (flusso di traffico)
- Istanze di policy di traffico (flusso di traffico)

Non tutte le risorse Route 53 supportano le autorizzazioni. Non puoi concedere o negare l'accesso alle risorse seguenti:

- Domini
- Singoli record
- Tag per domini
- Tag per i controlli dell'integrità
- Tag per hosted zone

Route 53 fornisce operazioni API per lavorare con ognuno di questi tipi di risorse. Per ulteriori informazioni, consulta il riferimento API di Amazon Route 53. Per un elenco di operazioni e l'ARN che specifichi per concedere o negare l'autorizzazione a utilizzare ciascuna operazione, consulta Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

Informazioni sulla proprietà delle risorse

Un AWS account possiede le risorse create nell'account, indipendentemente da chi le ha create. In particolare, il proprietario della risorsa è l' AWS account dell'entità principale (ovvero l'account root o un ruolo IAM) che autentica la richiesta di creazione delle risorse.

Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root del tuo AWS account per creare una zona ospitata, l' AWS account è il proprietario della risorsa.

- Se crei un utente nel tuo AWS account e concedi le autorizzazioni per creare una zona ospitata a quell'utente, l'utente può creare una zona ospitata. Tieni presente tuttavia che il tuo account AWS è il proprietario della risorsa della zona ospitata.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per creare una zona ospitata, chiunque possa assumere il ruolo può creare una zona ospitata. Il tuo AWS account, a cui appartiene il ruolo, possiede la risorsa della zona ospitata.

Gestione dell'accesso alle risorse

Una policy di autorizzazione specifica chi ha accesso a cosa. In questa sezione sono descritte le opzioni per la creazione di policy relative alle autorizzazioni per Amazon Route 53. Per informazioni generali sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Informazioni di riferimento sulle policy IAM AWS nella Guida per l'utente di IAM.

Le policy associate a un'identità IAM sono denominate policy basate su identità (policy IAM), mentre le policy associate a una risorsa sono denominate policy basate su risorsa. Route 53 supporta solo policy basate su identità (policy IAM).

Argomenti

Policy basate su identità (policy IAM)

Puoi collegare le policy alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Collega una policy di autorizzazione a un utente o a un gruppo nell'account: un amministratore account può utilizzare una policy di autorizzazione associata a un utente specifico per concedere autorizzazioni per tale utente al fine di creare risorse di Amazon Route 53.
- Associare una politica di autorizzazioni a un ruolo (concedere autorizzazioni per più account): è possibile concedere l'autorizzazione per eseguire azioni di Route 53 a un utente creato da un altro account. AWS Per farlo, puoi collegare una policy di autorizzazioni a un ruolo IAM e poi consentire all'utente nell'altro account di assumere il ruolo. L'esempio seguente spiega come questo funziona per due account AWS , account A e account B:
  1. L'amministratore dell'account A crea un ruolo IAM e lo collega a una policy di autorizzazioni che concede le autorizzazioni per creare o accedere alle risorse di proprietà dell'account A.

2. L'amministratore dell'account A attribuisce una policy di attendibilità al ruolo. La policy di attendibilità identifica l'account B come l'identità principale che può assumere il ruolo.
3. L'amministratore dell'account B può delegare le autorizzazioni di assumere il ruolo a qualsiasi degli utenti o gruppi nell'account B. In questo modo gli utenti nell'account B possono creare o accedere a risorse nell'account A.

Per ulteriori informazioni su come delegare le autorizzazioni agli utenti di un altro AWS account, consulta la sezione Gestione degli accessi nella IAM User Guide.

L'esempio di policy seguente consente a un utente di eseguire l'operazione `CreateHostedZone` per creare una zona ospitata pubblica per qualsiasi account AWS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Se desideri che la policy si applichi anche alle zone ospitate private, devi concedere le autorizzazioni per utilizzare l'`AssociateVPCWithHostedZone`azione Route 53 e due EC2 azioni Amazon `DescribeVpcs` e`DescribeRegion`, come mostrato nell'esempio seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource":"*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegion"
            ],
            "Resource":"*"
        },
    ]
}
```

Per ulteriori informazioni su come collegare policy alle identità per Route 53, consulta Utilizzo di policy basate su identità (policy IAM) per Amazon Route 53. Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consultare Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Anche altri servizi, come Amazon S3, supportano il collegamento di policy di autorizzazioni alle risorse. Ad esempio, è possibile associare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. Amazon Route 53 non supporta il collegamento di policy alle risorse.

Definizione degli elementi delle policy: risorse, operazioni, effetti ed entità principali

Amazon Route 53 include operazioni API (consulta la Documentazione di riferimento delle API di Amazon Route 53) utilizzabili per ciascuna risorsa Route 53 (consulta ARNs per le risorse Amazon Route 53). Puoi concedere a un utente o a un utente federato le autorizzazioni per eseguire una o tutte queste operazioni. Alcune operazioni API, ad esempio la registrazione di un dominio, richiedono le autorizzazioni per eseguire più di un'operazione.

Di seguito sono elencati gli elementi di base di una policy:

- Risorsa - Usa un Amazon Resource Name (ARN) per identificare la risorsa a cui si applica la policy. Per ulteriori informazioni, consulta ARNs per le risorse Amazon Route 53.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, a seconda dell'`Effect` specificato, l'autorizzazione `route53:CreateHostedZone` consente o rifiuta all'utente la possibilità di eseguire l'operazione `CreateHostedZone` di Route 53.
- Effetto - Specifichi l'effetto (autorizzazione o rifiuto) quando un utente prova a eseguire l'operazione sulla risorsa specificata. Se non concedi esplicitamente l'accesso a un'operazione, l'accesso viene

implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.

- Principale - Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). Route 53 non supporta le policy basate su risorse.

Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Informazioni di riferimento sulle policy IAM AWS nella Guida per l'utente di IAM.

Per un elenco che riporta tutte le operazioni API di Route 53 e le risorse a cui si applicano, consulta Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

Specifica delle condizioni in una policy

Quando si concedono le autorizzazioni, è possibile utilizzare il linguaggio della policy IAM per specificare quando la policy deve essere applicata. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta Elementi delle policy JSON IAM: Condizione nella Guida per l'utente di IAM.

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per Route 53. Tuttavia, ci sono AWS ampie chiavi condizionali che puoi utilizzare in base alle tue esigenze. Per un elenco completo delle chiavi AWS ampie, consulta Available keys for conditions nella IAM User Guide.

Utilizzo di policy basate su identità (policy IAM) per Amazon Route 53

In questo argomento sono forniti esempi di policy basate su identità che illustrano come un amministratore account può collegare policy di autorizzazioni a identità IAM e quindi concedere autorizzazioni per eseguire operazioni sulle risorse di Amazon Route 53.

> **Important**
>
> In primo luogo, è consigliabile esaminare gli argomenti introduttivi in cui vengono spiegati i concetti di base e le opzioni per gestire l'accesso alle risorse Route 53. Per ulteriori informazioni, consulta Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Route 53.

> **Note**
>
> Quando si concede l'accesso, la zona ospitata e Amazon VPC devono appartenere alla stessa partizione. Una partizione è un gruppo di. Regioni AWS Ciascuno Account AWS è limitato a una partizione.
> Di seguito sono riportate le partizioni supportate:
>
> - `aws` - Regioni AWS
> - `aws-cn`: Regioni Cina
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> Per ulteriori informazioni, consulta Gestione dell'accesso ed Endpoint e quote di Amazon Route 53 nella Guida di riferimento generale di AWS .

Argomenti

- Autorizzazioni necessarie per utilizzare la console Amazon Route 53
- Autorizzazioni di esempio per il proprietario di un record di dominio
- Autorizzazioni delle chiavi gestite dal cliente di Route 53 richieste per la firma DNSSEC
- Esempi di policy gestite dal cliente

Di seguito viene illustrato un esempio di policy di autorizzazione. Il `Sid`, o ID dichiarazione, è facoltativo:

```
{
    "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": "*"
        }
    ]
}
```

La policy include due dichiarazioni:

- La prima dichiarazione consente di concedere autorizzazioni per le azioni necessarie per creare e gestire zone ospitate pubbliche e i relativi record. Il carattere jolly (*) nell'Amazon Resource Name (ARN) consente l'accesso a tutte le zone ospitate di proprietà dell'account corrente. AWS
- La seconda dichiarazione consente di concedere autorizzazioni per tutte le azioni necessarie per creare e gestire i controlli dell'integrità.

Per un elenco di operazioni e l'ARN che specifichi per concedere o negare l'autorizzazione a utilizzare ciascuna operazione, consulta Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

Autorizzazioni necessarie per utilizzare la console Amazon Route 53

Per concedere l'accesso completo alla console Amazon Route 53 è necessario concedere le autorizzazioni nelle seguenti policy di autorizzazione:

```
{
    "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"
        }
    ]
}
```

Di seguito viene descritto perché le autorizzazioni sono necessarie:

`route53:*`

Consente di eseguire tutte le operazioni di Route 53, tranne le seguenti:

- Crea e aggiorna record di alias per i quali il valore di Alias Target è una CloudFront distribuzione, un sistema di bilanciamento del carico Elastic Load Balancing, un ambiente Elastic Beanstalk o un bucket Amazon S3. Con queste autorizzazioni, puoi creare record alias per cui il valore di Alias Target (Destinazione alias) è un altro record nella stessa hosted zone.
- Utilizzare le zone ospitate private.
- Lavorare con i domini.
- Crea, elimina e visualizza gli allarmi. CloudWatch
- Esegui il rendering CloudWatch delle metriche nella console Route 53.

`route53domains:*`

Consente di lavorare con domini.

> **Important**
>
> Se si elencano operazioni `route53` individualmente, è necessario includere `route53:CreateHostedZone` per lavorare con domini. Quando si registra un dominio, una zona ospitata viene creata nello stesso momento, quindi una policy che include le autorizzazioni per registrare domini, inoltre, richiede il permesso di creare hosted zone.

Per la registrazione di domini, Route 53 non supporta la concessione o il rifiuto di autorizzazioni per singole risorse.

`route53resolver:*`

Consente di lavorare con Route 53 Resolver.

`ssm:GetParametersByPath`

Consente di recuperare regioni disponibili pubblicamente quando crei nuovi record alias, zone ospitate private e controlli dell'integrità.

`cloudfront:ListDistributions`

Consente di creare e aggiornare record di alias per i quali il valore di Alias Target è una distribuzione. CloudFront

Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di distribuzioni da visualizzare nella console.

`elasticloadbalancing:DescribeLoadBalancers`

Consente di creare e aggiornare i record alias per cui il valore di Alias Target (Destinazione alias) è un load balancer ELB.

Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di bilanciatori del carico da visualizzare nella console.

`elasticbeanstalk:DescribeEnvironments`

Consente di creare e aggiornare i record alias per cui il valore di Destinazione alias è un ambiente Elastic Beanstalk.

Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di ambienti da visualizzare nella console.

`s3:ListAllMyBuckets`, **`s3:GetBucketLocation`** e **`s3:GetBucketWebsite`**

Consente di creare e aggiornare i record alias per cui il valore di Destinazione alias è un bucket Amazon S3. (Puoi creare un alias per un bucket Amazon S3 solo se il bucket è configurato come endpoint di sito Web; `s3:GetBucketWebsite` ottiene le informazioni richieste sulla configurazione).

Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di bucket da visualizzare nella console.

`ec2:DescribeVpcs` e **`ec2:DescribeRegions`**

Consente di lavorare con zone ospitate private.

Tutte le autorizzazioni **`ec2`** elencate

Consente di lavorare con Route 53 Resolver.

`sns:ListTopics`, **`sns:ListSubscriptionsByTopic`**, **`sns:CreateTopic`**, **`cloudwatch:DescribeAlarms`**, **`cloudwatch:PutMetricAlarm`**, **`cloudwatch:DeleteAlarms`**

Consente di creare, eliminare e visualizzare CloudWatch gli allarmi.

`cloudwatch:GetMetricStatistics`

Consente di creare controlli CloudWatch metrici dello stato.

Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere statistiche da visualizzare nella console.

`apigateway:GET`

Consente di creare e aggiornare i record alias per i quali il valore di Destinazione alias è un'API di Amazon API Gateway.

Questa autorizzazione non è necessaria se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di APIs cose da visualizzare nella console.

`kms:*`

Consente di utilizzare AWS KMS per abilitare la firma DNSSEC.

Autorizzazioni di esempio per il proprietario di un record di dominio

Con le autorizzazioni relative al set di record di risorse è possibile impostare autorizzazioni granulari che limitano ciò che l' AWS utente può aggiornare o modificare. Per ulteriori informazioni, consulta Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi.

In alcuni scenari, il proprietario di una zona ospitata potrebbe essere responsabile della gestione complessiva della zona ospitata mentre un'altra persona dell'organizzazione è responsabile di un sottoinsieme di tali attività. Il proprietario di una zona ospitata che ha abilitato la firma DNSSEC, ad esempio, potrebbe voler creare una policy IAM che includa l'autorizzazione di qualcun altro ad aggiungere ed eliminare Resource Set Records (RRs) nella zona ospitata, tra le altre attività. Le autorizzazioni specifiche che il proprietario di una zona ospitata sceglie di abilitare per un proprietario di record o altri utenti dipenderanno dalle policy dell'organizzazione.

Di seguito è riportato un esempio di policy IAM che consente al proprietario di un record di apportare modifiche alle RRs politiche di traffico e ai controlli di integrità. Un proprietario di record con questa policy non può eseguire operazioni a livello di zona, ad esempio la creazione o l'eliminazione di una

zona, l'abilitazione o la disabilitazione della registrazione delle query, la creazione o l'eliminazione di un set di delega riutilizzabile o la modifica delle impostazioni DNSSEC.

```
{
      "Sid": "Do not allow zone-level modification ",
      "Effect": "Allow",
      "Action": [
        "route53:ChangeResourceRecordSets",
        "route53:CreateTrafficPolicy",
        "route53:DeleteTrafficPolicy",
        "route53:CreateTrafficPolicyInstance",
        "route53:CreateTrafficPolicyVersion",
        "route53:UpdateTrafficPolicyInstance",
        "route53:UpdateTrafficPolicyComment",
        "route53:DeleteTrafficPolicyInstance",
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:List*",
        "route53:Get*"
      ],
      "Resource": [
        "*"
      ]
}
```

Autorizzazioni delle chiavi gestite dal cliente di Route 53 richieste per la firma DNSSEC

Quando abiliti la firma DNSSEC per Route 53, Route 53 crea una chiave di firma delle chiavi (KSK) basata su una chiave gestita dal cliente (). AWS Key Management Service AWS KMS Puoi usare una chiave gestita dal cliente esistente che supporti la firma DNSSEC o crearne una nuova. Perché possa creare una KSK per tuo conto, Route 53 deve poter accedere alla chiave gestita dal cliente.

Per abilitare Route 53 per accedere alla chiave gestita dal cliente, assicurati che la policy della chiave gestita dal cliente contenga le seguenti istruzioni:

```
{
            "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
                }
            }
        }
```

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Per proteggervi AWS KMS da tale problema, potete facoltativamente limitare le autorizzazioni di cui un servizio dispone per una risorsa in una politica basata sulle risorse, fornendo una combinazione di e condizioni (entrambe o una). `aws:SourceAccount` `aws:SourceArn` `aws:SourceAccount`è l'ID AWS dell'account del proprietario di una zona ospitata. `aws:SourceArn`è un ARN di una zona ospitata.

Di seguito sono riportati due esempi di autorizzazioni che è possibile aggiungere:

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
```

```
    }
},
```

- O -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

Per ulteriori informazioni, consultare Problema del "confused deputy" nella Guida per l'utente di IAM.

Esempi di policy gestite dal cliente

Puoi creare le tue policy IAM personalizzate per consentire autorizzazioni per le operazioni di Route 53. È possibile allegare queste policy personalizzate ai gruppi IAM che hanno bisogno delle autorizzazioni specificate. Queste politiche funzionano quando si utilizza l'API Route 53 AWS SDKs, o la AWS CLI. I seguenti esempi mostrano le autorizzazioni per diversi casi d'uso comuni. Per la policy che concede a un utente accesso completo a Route 53, consulta Autorizzazioni necessarie per utilizzare la console Amazon Route 53.

Esempi

- Esempio 1: Consentire l'accesso in lettura a tutte le zone ospitate
- Esempio 2: Consentire la creazione ed eliminazione delle zone ospitate
- Esempio 3: Consentire l'accesso completo a tutti i domini (solo zone ospitate pubbliche)
- Esempio 4: Consentire la creazione di endpoint di Route 53 Resolver in entrata e in uscita

Esempio 1: Consentire l'accesso in lettura a tutte le zone ospitate

La seguente policy di autorizzazione concede all'utente le autorizzazioni per elencare tutte le zone ospitate e visualizzare tutti i record in una zona ospitata.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

Esempio 2: Consentire la creazione ed eliminazione delle zone ospitate

La seguente policy di autorizzazione consente agli utenti di creare e cancellare zone ospitate e di monitorare l'avanzamento della modifica.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
```

```
}
```

Esempio 3: Consentire l'accesso completo a tutti i domini (solo zone ospitate pubbliche)

La seguente policy di autorizzazione consente agli utenti di eseguire tutte le azioni su registrazioni di dominio, incluse le autorizzazioni per registrare domini e creare hosted zone.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Quando si registra un dominio, una zona ospitata viene creata nello stesso momento, quindi una policy che include le autorizzazioni per registrare domini, inoltre, richiede le autorizzazioni per creare hosted zone. (Per la registrazione di domini, Route 53 non supporta la concessione di autorizzazioni per singole risorse.)

Per informazioni sulle autorizzazioni necessarie per lavorare con zone ospitate private, consulta Autorizzazioni necessarie per utilizzare la console Amazon Route 53.

Esempio 4: Consentire la creazione di endpoint di Route 53 Resolver in entrata e in uscita

La policy di autorizzazioni riportata di seguito consente agli utenti di utilizzare la console Route 53 per creare endpoint in ingresso e in uscita di Resolver.

Alcune di queste autorizzazioni sono necessarie solo per creare endpoint nella console. È possibile omettere queste autorizzazioni se si desidera concedere autorizzazioni solo per creare endpoint in ingresso e in uscita a livello di codice:

- `route53resolver:ListResolverEndpoints` consente agli utenti di visualizzare l'elenco degli endpoint in ingresso o in uscita in modo da poter verificare che sia stato creato un endpoint.

- `DescribeAvailabilityZones` è necessario per visualizzare un elenco di Zone di disponibilità.
- `DescribeVpcs`è necessario per visualizzare un elenco di. VPCs

```
{
    "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": "*"
        }
    ]
}
```

Utilizzo di ruoli collegati ai servizi per Amazon Route 53 Resolver

Route 53 Resolver utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente a Resolver. I ruoli collegati ai servizi sono predefiniti da Resolver e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di Resolver perché ti permette di evitare l'aggiunta manuale delle autorizzazioni necessarie. Resolver definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, solo Resolver potrà assumere i suoi ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di Resolver perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- Autorizzazioni del ruolo collegato ai servizi per Resolver
- Creazione di un ruolo collegato ai servizi per Resolver
- Modifica di un ruolo collegato ai servizi per Resolver
- Eliminazione di un ruolo collegato ai servizi per Resolver
- Regioni supportate per i ruoli collegati ai servizi di Resolver

Autorizzazioni del ruolo collegato ai servizi per Resolver

Resolver utilizza la il ruolo collegato ai servizi **`AWSServiceRoleForRoute53Resolver`**per recapitare log di query per tuo conto.

La policy delle autorizzazioni del ruolo consente a Resolver di eseguire le operazioni riportate di seguito su tutte le risorse:

```
{
  "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": "*"
    }
  ]
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Resolver

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un'associazione di configurazione del registro di interrogazione del resolver nella console Amazon Route 53, o nell' AWS API AWS CLI, Resolver crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Se inoltre usavi il servizio Resolver prima del 12 agosto 2020, data da cui è disponibile il supporto dei ruoli collegati ai servizi, allora Resolver ha creato il ruolo `AWSServiceRoleForRoute53Resolver` nel tuo account. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei una nuova associazione di configurazione del log di query del resolver, il ruolo collegato ai servizi `AWSServiceRoleForRoute53Resolver` viene creato nuovamente per tuo conto.

Modifica di un ruolo collegato ai servizi per Resolver

Resolver non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForRoute53Resolver`. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per Resolver

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio Resolver utilizza tale ruolo quando provi a eliminare le risorse, è possibile che l'eliminazione abbia esito negativo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Come eliminare le risorse di Resolver utilizzate da **`AWSServiceRoleForRoute53Resolver`**

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Espandi il menu della console Route 53. Nell'angolo in alto a sinistra della console, scegli l'icona con le tre barre orizzontali (☰).
3. Nel menu Resolver, scegli Registrazione delle query.
4. Seleziona la casella di controllo accanto al nome della configurazione di registrazione delle query, quindi scegli Elimina.
5. Nella casella di testo Elimina configurazione di registrazione delle query seleziona Interrompi registrazione delle query.

   Questa operazione dissocerà la configurazione dal VPC. Puoi dissociare la configurazione della registrazione delle query anche a livello di programmazione. Per ulteriori informazioni, consulta disassociate-resolver-query-log-config.
6. Dopo che la registrazione delle query è stata interrotta, se lo desideri puoi digitare **`delete`** nel campo e scegliere Elimina per eliminare la configurazione di registrazione delle query. Tuttavia, ciò non è necessario per eliminare le risorse utilizzate da `AWSServiceRoleForRoute53Resolver`.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al `AWSServiceRoleForRoute53Resolver` servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Resolver

Resolver non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. Il ruolo `AWSServiceRoleForRoute53Resolver` può essere utilizzato nelle regioni seguenti.

Nome della Regione	Identità della regione	Supporto per Resolver
US East (N. Virginia)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
US West (N. California)	us-west-1	Sì
US West (Oregon)	us-west-2	Sì
Asia Pacific (Mumbai)	ap-south-1	Sì
Asia Pacifico (Osaka-Locale)	ap-northeast-3	Sì
Asia Pacifico (Seul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Canada (Central)	ca-central-1	Sì
Europe (Frankfurt)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Europe (London)	eu-west-2	Sì
Europe (Paris)	eu-west-3	Sì
Sud America (São Paulo)	sa-east-1	Sì
China (Beijing)	cn-north-1	Sì

Nome della Regione	Identità della regione	Supporto per Resolver
Cina (Ningxia)	cn-northwest-1	Sì
AWS GovCloud (US)	us-gov-east-1	Sì
AWS GovCloud (US)	us-gov-west-1	Sì

AWS politiche gestite per Amazon Route 53

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AmazonRoute 53 FullAccess

È possibile allegare la policy `AmazonRoute53FullAccess` alle identità IAM.

Questa policy concede l'accesso completo alle risorse Route 53, inclusa la registrazione del dominio e il controllo dell'integrità, ma escludendo Resolver.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53:*`: consente di eseguire tutte le operazioni di Route 53, tranne le seguenti:

  - Crea e aggiorna record di alias per i quali il valore di Alias Target è una CloudFront distribuzione, un sistema di bilanciamento del carico Elastic Load Balancing, un ambiente Elastic Beanstalk o un bucket Amazon S3. Con queste autorizzazioni, puoi creare record alias per cui il valore di Alias Target (Destinazione alias) è un altro record nella stessa hosted zone.
  - Utilizzare le zone ospitate private.
  - Lavorare con i domini.
  - Crea, elimina e visualizza gli allarmi. CloudWatch
  - Esegui il rendering CloudWatch delle metriche nella console Route 53.
- `route53domains:*`: consente di lavorare con i domini.
- `cloudfront:ListDistributions`— Consente di creare e aggiornare record di alias per i quali il valore di Alias Target è una distribuzione. CloudFront

  Questa autorizzazione non è necessaria se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di distribuzioni da visualizzare nella console.
- `elasticloadbalancing:DescribeLoadBalancers`: consente di creare e aggiornare i record alias per cui il valore di Destinazione alias è un load balancer Elastic Load Balancing.

  Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di bilanciatori del carico da visualizzare nella console.
- `elasticbeanstalk:DescribeEnvironments`: consente di creare e aggiornare i record alias per cui il valore di Destinazione alias è un ambiente Elastic Beanstalk.

  Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di ambienti da visualizzare nella console.
- `s3:ListBucket`, `s3:GetBucketLocation` e `s3:GetBucketWebsite`: consente di creare e aggiornare i record alias per cui il valore di Destinazione alias è un bucket Amazon S3. (Puoi creare un alias per un bucket Amazon S3 solo se il bucket è configurato come endpoint di sito Web; `s3:GetBucketWebsite` ottiene le informazioni richieste sulla configurazione).

  Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di bucket da visualizzare nella console.
- `ec2:DescribeVpcs`— Consente di visualizzare un elenco di. VPCs
- `ec2:DescribeVpcEndpoints`: consente di visualizzare un elenco di endpoint VPC.
- `ec2:DescribeRegions`: consente di visualizzare un elenco di zone di disponibilità.

- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Consente di creare, eliminare e visualizzare CloudWatch allarmi.
- `cloudwatch:GetMetricStatistics`— Consente di creare controlli sanitari CloudWatch metrici.

  Queste autorizzazioni non sono necessarie se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere statistiche da visualizzare nella console.
- `apigateway:GET`: consente di creare e aggiornare i record alias per i quali il valore di Destinazione alias è un'API di Amazon API Gateway.

  Questa autorizzazione non è necessaria se non utilizzi la console Route 53. Route 53 lo utilizza solo per ottenere un elenco di APIs cose da visualizzare nella console.

Per ulteriori informazioni sulle autorizzazioni, consultaAutorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

```
{
    "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 politica gestita: 53 AmazonRoute ReadOnlyAccess

È possibile allegare la policy `AmazonRoute53ReadOnlyAccess` alle identità IAM.

Questa policy concede l'accesso in sola lettura alle risorse Route 53, inclusa la registrazione del dominio e il controllo dell'integrità, ma escludendo Resolver.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53:Get*_` ottiene le risorse Route 53.
- `route53:List*`: elenca le risorse Route 53.
- `route53:TestDNSAnswer`: ottiene il valore restituito da Route 53 in risposta a una richiesta DNS.

Per ulteriori informazioni sulle autorizzazioni, vedereAutorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: 53 AmazonRoute DomainsFullAccess

È possibile allegare la policy `AmazonRoute53DomainsFullAccess` alle identità IAM.

Questa policy consente l'accesso completo alle risorse di registrazione dei domini Route 53.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53:CreateHostedZone`: consente di creare una zona ospitata Route 53.
- `route53domains:*`: consente di registrare nomi di dominio ed eseguire le operazioni correlate.

Per ulteriori informazioni sulle autorizzazioni, vedereAutorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: 53 AmazonRoute DomainsReadOnlyAccess

È possibile allegare la policy `AmazonRoute53DomainsReadOnlyAccess` alle identità IAM.

Questa policy consente l'accesso in sola lettura alle risorse di registrazione dei domini Route 53.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53domains:Get*`: consente di recuperare un elenco di domini da Route 53.
- `route53domains:List*`: consente di visualizzare un elenco di domini Route 53.

Per ulteriori informazioni sulle autorizzazioni, vedereAutorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: 53 AmazonRoute ResolverFullAccess

È possibile allegare la policy `AmazonRoute53ResolverFullAccess` alle identità IAM.

Questa policy concede l'accesso completo alle risorse di Route 53 Resolver.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53resolver:*`: consente di creare e gestire risorse di Resolver sulla console Route 53.
- `ec2:DescribeSubnets`: consente di elencare le sottoreti di Amazon VPC.
- `ec2:CreateNetworkInterface`, `ec2:DeleteNetworkInterface`, e `ec2:ModifyNetworkInterfaceAttribute`: consente di creare, modificare ed eliminare le interfacce di rete.
- `ec2:DescribeNetworkInterfaces`: consente di visualizzare un elenco di interfacce di rete.
- `ec2:DescribeSecurityGroups`: consente di visualizzare un elenco di tutti i gruppi di sicurezza.

- `ec2:DescribeVpcs`— Consente di visualizzare un elenco di VPCs.
- `ec2:DescribeAvailabilityZones`: consente di elencare le zone disponibili.

Per ulteriori informazioni sulle autorizzazioni, vedereAutorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: 53 AmazonRoute ResolverReadOnlyAccess

È possibile allegare la policy `AmazonRoute53ResolverReadOnlyAccess` alle identità IAM.

Questa policy concede l'accesso in sola lettura alle risorse di Route 53 Resolver.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53resolver:Get*`— Ottiene risorse Resolver.

- `route53resolver:List*`: consente di visualizzare un elenco delle risorse del Resolver.
- `ec2:DescribeNetworkInterfaces`: consente di visualizzare un elenco di interfacce di rete.
- `ec2:DescribeSecurityGroups`: consente di visualizzare un elenco di tutti i gruppi di sicurezza.

Per ulteriori informazioni sulle autorizzazioni, vedere. Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: Route53 ResolverServiceRolePolicy

Non è possibile collegare `Route53ResolverServiceRolePolicy`alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Route 53 Resolver di accedere ai servizi AWS e alle risorse utilizzati o gestiti da Resolver. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Route 53 Resolver.

AWS politica gestita: 53 AmazonRoute ProfilesFullAccess

È possibile allegare la policy `AmazonRoute53ProfilesReadOnlyAccess` alle identità IAM.

Questa politica garantisce l'accesso completo alle risorse del profilo Amazon Route 53.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `route53profiles`— Consente di creare e gestire le risorse del profilo sulla console Route 53.
- `ec2`— Consente ai responsabili di ottenere informazioni su VPCs.

Per ulteriori informazioni sulle autorizzazioni, vedere. Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:PutProfilePolicy",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
```

```
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS politica gestita: 53 AmazonRoute ProfilesReadOnlyAccess

È possibile allegare la policy `AmazonRoute53ProfilesReadOnlyAccess` alle identità IAM.

Questa policy garantisce l'accesso in sola lettura alle risorse del profilo Amazon Route 53.

Dettagli dell'autorizzazione

Per ulteriori informazioni sulle autorizzazioni, consulta. Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig"
            ],
            "Resource": [
                "*"
            ]
```

```
        }
    ]
}
```

Route 53 aggiorna le politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Route 53 da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti di Route 53.

Modifica	Descrizione	Data
AmazonRoute53 ProfilesFullAccess — Politica aggiornata	Aggiunge le autorizzazioni per `GetProfilePolicy` e `PutProfilePolicy` . Si tratta di operazioni IAM che richiedono solo l'autorizzazione. Se a un preside IAM non sono concesse queste autorizzazioni, si verificherà un errore durante il tentativo di condividere il profilo utilizzando il servizio. AWS RAM	27 agosto 2024
AmazonRoute53 ProfilesReadOnlyAccess — Politica aggiornata	Aggiunge le autorizzazioni per `GetProfilePolicy` . Questa è un'azione IAM che richiede solo l'autorizzazione. Se a un principale IAM non viene concessa questa autorizzazione, si verificherà un errore nel tentativo di accedere alla politica del profilo utilizzando il servizio. AWS RAM	27 agosto 2024

Modifica	Descrizione	Data
AmazonRoute53 ResolverFullAccess — Politica aggiornata	È stato aggiunto un ID di dichiarazione (Sid) per identificare in modo univoco la politica.	5 agosto 2024
AmazonRoute53 ResolverReadOnlyAccess — Politica aggiornata	È stato aggiunto un ID di dichiarazione (Sid) per identificare in modo univoco la politica.	5 agosto 2024
AmazonRoute53 ProfilesFullAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso completo alle risorse del profilo Amazon Route 53.	22 aprile 2024
AmazonRoute53 ProfilesReadOnlyAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso in sola lettura alle risorse del profilo Amazon Route 53.	22 aprile 2024
Route53: nuova politica ResolverServiceRolePolicy	Amazon Route 53 ha aggiunto una nuova policy associata a un ruolo collegato ai servizi che consente a Route 53 Resolver di accedere a AWS servizi e risorse utilizzati o gestiti da Resolver.	14 luglio 2021
AmazonRouteResolverReadOnlyAccess53 — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso in sola lettura alle risorse Route 53 Resolver.	14 luglio 2021

Modifica	Descrizione	Data
AmazonRoute53 — Nuova politica ResolverFullAccess	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso completo alle risorse di Route 53 Resolver.	14 luglio 2021
AmazonRoute53 DomainsReadOnlyAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso in sola lettura alle risorse dei domini Route 53.	14 luglio 2021
AmazonRoute53 DomainsFullAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso completo alle risorse dei domini Route 53.	14 luglio 2021
AmazonRoute53 ReadOnlyAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso in sola lettura alle risorse Route 53.	14 luglio 2021
AmazonRoute53 FullAccess — Nuova politica	Amazon Route 53 ha aggiunto una nuova policy per consentire l'accesso completo alle risorse Route 53.	14 luglio 2021
Route 53 ha iniziato il monitoraggio delle modifiche	Route 53 ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	14 luglio 2021

Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi

In Route 53 puoi specificare le condizioni durante la concessione delle autorizzazioni utilizzando una policy IAM (consulta Controllo accessi). Ad esempio, puoi:

- Concedi le autorizzazioni per consentire l'accesso a un singolo set di record di risorse.

- Concedi le autorizzazioni per consentire agli utenti di accedere a tutti i set di record di risorse di un tipo di record DNS specifico in una zona ospitata, ad esempio i record A e AAAA.
- Concedi le autorizzazioni per consentire agli utenti di accedere a un set di record di risorse in cui il nome contiene una stringa specifica.
- Concedi le autorizzazioni per consentire agli utenti di eseguire solo un sottoinsieme delle `CREATE | UPSERT | DELETE` azioni sulla console Route 53 o quando utilizzano l'API. ChangeResourceRecordSets
- Concedi le autorizzazioni per consentire agli utenti di associare o dissociare zone ospitate private da un particolare VPC.
- Concedi le autorizzazioni per consentire agli utenti di elencare le zone ospitate associate a un particolare VPC.
- Concedi le autorizzazioni per consentire agli utenti di accedere per creare una nuova zona ospitata privata e associarla a un particolare VPC.
- Concedi le autorizzazioni per consentire agli utenti di creare o eliminare un'autorizzazione di associazione VPC.

Puoi anche creare autorizzazioni che combinano tutte le autorizzazioni granulari.

Normalizzazione dei valori chiave della condizione Route 53

I valori inseriti per le condizioni della policy devono essere formattati o normalizzati come segue:

Per **`route53:ChangeResourceRecordSetsNormalizedRecordNames`**:

- Tutte le lettere devono essere minuscole.
- Il nome DNS non deve avere un punto finale.
- I caratteri diversi da a-z, 0-9, - (trattino), _ (trattino basso) e . (punto, come delimitatore tra le etichette) devono utilizzare i codici escape nel formato \codice ottale a tre cifre. Ad esempio, `\052` è il codice ottale per il carattere *.

Per **`route53:ChangeResourceRecordSetsActions`**, il valore può essere uno dei seguenti e deve essere in maiuscolo:

- CREATE
- UPSERT
- DELETE

Per **`route53:ChangeResourceRecordSetsRecordTypes`**:

- Il valore deve essere in maiuscolo e può essere uno qualsiasi dei tipi di record DNS supportati da Route 53. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

Per **`route53:VPCs`**:

- Il valore deve essere nel formato di`VPCId=<vpc-id>,VPCRegion=<region>`.
- Il valore di `<vpc-id>` e `<region>` deve essere in lettere minuscole, ad esempio e`VPCId=vpc-123abc`. `VPCRegion=us-east-1`
- Le chiavi e i valori di contesto fanno distinzione tra maiuscole e minuscole.

> **Important**
>
> Affinché le tue autorizzazioni consentano o limitino le azioni come desideri, devi seguire queste convenzioni. Solo `VPCId` gli `VPCRegion` elementi sono accettati da questa chiave di condizione, tutte AWS le altre risorse, ad esempio Account AWS, non sono supportate.

Puoi utilizzare l'Analizzatore di accessi o il Simulatore di policy nella Guida per l'utente di IAM per accertarti che la policy conceda o limiti le autorizzazioni come previsto. Puoi verificare le autorizzazioni anche applicando una policy IAM a un utente o ruolo di test che esegua le operazioni di Route 53.

Specifica delle condizioni: uso delle chiavi di condizione

AWS fornisce un set di chiavi di condizione predefinite (chiavi di condizione AWS-wide) per tutti i AWS servizi che supportano IAM per il controllo degli accessi. Ad esempio, puoi utilizzare la chiave di condizione `aws:SourceIp` per controllare l'indirizzo IP del richiedente prima che un'operazione venga effettuata. Per ulteriori informazioni e per un elenco completo delle chiavi AWS generiche, consulta Chiavi disponibili per le condizioni nella Guida per l'utente di IAM.

> **Note**
>
> Route 53 non supporta le chiavi di condizione basate su tag.

La tabella seguente mostra le chiavi di condizione specifiche del servizio Route 53 che si applicano a Route 53.

Chiave di condizione di Route 53	Operazioni API	Value type (Tipo di valore)	Descrizione
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	Multivalore	Rappresenta un elenco di nomi di record DNS nella richiesta di. ChangeResourceRecordSets Per ottenere il comportamento previsto, i nomi DNS nella policy IAM devono essere normalizzati come segue: • Tutte le lettere devono essere minuscole. • Il nome DNS non deve avere un punto finale. • I caratteri diversi da a-z, 0-9, - (trattino), _ (trattino basso) e . (punto, come delimitatore tra le etichette) devono utilizzare i codici escape nel formato \codice ottale a tre cifre.
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	Multivalore	Rappresenta un elenco di tipi di record DNS nella richiesta di `ChangeResourceRecordSets` . `ChangeResourceRecordSetsRecordTypes` può essere uno qualsiasi dei tipi di record DNS supportati da Route 53. Per ulteriori informazioni, consulta Tipi di record DNS supportati. Quanto riportato nella policy deve essere tutto maiuscolo.
`route53:ChangeResourceRecor`	ChangeResourceRecordSets	Multivalore	Rappresenta un elenco di operazioni nella richiesta di `ChangeResourceRecordSets` .

Chiave di condizione di Route 53	Operazioni API	Value type (Tipo di valore)	Descrizione
`dSetsActions`			`ChangeResourceRecordSetsActions` può essere uno dei seguenti valori (deve essere in maiuscolo): • CREATE • UPSERT • DELETE

Chiave di condizione di Route 53	Operazioni API	Value type (Tipo di valore)	Descrizione
`route53:VPCs`	Associare VPCWith HostedZone Dissociarsi VPCFrom HostedZone ListHosteddZonesByVPC CreateHostedZone Crea autorizzazione VPCAssociation VPCAssociationAutorizzazione di eliminazione	Multivalore	Rappresenta un elenco di VPCs nella richiesta di `AssociateVPCWithHostedZone DisassociateVPCFromHostedZone` , `ListHostedZonesByVPC CreateHostedZone` ,`CreateVPCAssociationAuthorization` ,, `eDeleteVPCAssociationAuthorization` , nel formato "VPCId=<vpc-id>, VPCRegion = <region>

Policy di esempio: utilizzo di condizioni per l'accesso granulare

Ognuno degli esempi presenti in questa sezione imposta la clausola Effect su Allow (Consenti) e specifica solo le operazioni, le risorse e i parametri permessi. L'accesso è consentito solo a ciò che è elencato esplicitamente nella policy IAM.

In alcuni casi è possibile riscrivere queste policy in modo che si basino sul rifiuto (vale a dire impostare la clausola Effect su Deny e invertire tutta la logica nella policy). Tuttavia, ti consigliamo

di evitare di utilizzare le policy basate sul rifiuto poiché sono difficili da scrivere correttamente in confronto alle policy basate sul permesso. Ciò è particolarmente vero per Route 53 a causa della normalizzazione del testo che è richiesta.

Concessione delle autorizzazioni che limitano l'accesso ai record DNS con nomi specifici

La seguente policy di autorizzazione concede le autorizzazioni che consentono operazioni `ChangeResourceRecordSets` sulla zona ospitata Z12345 per example.com e marketing.example.com. Utilizza la chiave di condizione `route53:ChangeResourceRecordSetsNormalizedRecordNames` per limitare le azioni dell'utente solo sui record che corrispondono ai nomi specificati.

```
{
    "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` è un operatore di condizioni IAM che si applica alle chiavi con più valori. La condizione indicata nella policy precedente consentirà l'operazione solo quando tutte le modifiche apportate in `ChangeResourceRecordSets` hanno il nome DNS di esempio.com. Per ulteriori informazioni, consulta Operatori di condizione IAM e Condizione IAM con più chiavi o valori nella Guida per l'utente di IAM.

Per implementare l'autorizzazione che abbina i nomi a determinati suffissi, puoi utilizzare il carattere jolly IAM (*) nella policy con operatore di condizione `StringLike` o `StringNotLike`. La seguente policy consentirà l'operazione quando tutte le modifiche apportate nell'operazione `ChangeResourceRecordSets` ha nomi DNS che terminano con "-beta.esempio.com".

```
{
```

```
    "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**
>
> Il carattere jolly IAM non è uguale al carattere jolly del nome di dominio. Consulta il seguente esempio per informazioni su come utilizzare il carattere jolly con un nome di dominio.

Concedi autorizzazioni che limitano l'accesso ai record DNS che corrispondono a un nome di dominio contenente un carattere jolly

La seguente policy di autorizzazione concede le autorizzazioni che consentono operazioni `ChangeResourceRecordSets` sulla zona ospitata Z12345 per esempio.com. Utilizza la chiave di condizione `route53:ChangeResourceRecordSetsNormalizedRecordNames` per limitare le azioni dell'utente solo ai record che corrispondono a *.esempio.com.

```
{
    "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` è il codice ottale per il carattere * nel nome DNS, e \ in `\052` è sottoposto a escape in modo da essere \\ per seguire la sintassi JSON.

Concessione delle autorizzazioni che limitano l'accesso a record DNS specifici

La seguente policy di autorizzazione concede le autorizzazioni che consentono operazioni `ChangeResourceRecordSets` sulla zona ospitata Z12345 per esempio.com. Utilizza la combinazione di tre chiavi di condizione per limitare le azioni dell'utente e consentire solo la creazione o la modifica di record DNS con determinati nomi e tipi DNS.

```
{
    "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"]
                }
            }
          }
        ]
}
```

Concessione delle autorizzazioni che limitano l'accesso alla creazione e alla modifica dei soli tipi di record DNS specificati

La seguente policy di autorizzazione concede le autorizzazioni che consentono operazioni `ChangeResourceRecordSets` sulla zona ospitata Z12345 per esempio.com. Utilizza la chiave di condizione `route53:ChangeResourceRecordSetsRecordTypes` per limitare le azioni dell'utente solo sui record che corrispondono ai tipi specificati (A e AAAA).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
            }
          }
        ]
}
```

Concedi autorizzazioni che specificano il VPC in cui il principale IAM può operare

La seguente politica di autorizzazioni concede autorizzazioni che consentonoAssociateVPCWithHostedZone,, DisassociateVPCFromHostedZone ListHostedZonesByVPC CreateHostedZoneCreateVPCAssociationAuthorization, e DeleteVPCAssociationAuthorization azioni sul VPC specificato da vpc-id.

> **Important**
>
> Il valore della condizione deve essere nel formato di. VPCId=<vpc-id>,VPCRegion=<region> Se si specifica un ARN VPC nel valore della condizione, la chiave di condizione non avrà effetto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "route53:*"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "ForAllValues:StringLike": {
                    "route53:VPCs": [
                        "VPCId=<vpc-id>,VPCRegion=<region>"
                    ]
                }
            }
        },
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcs",
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni API di Amazon Route 53: riferimento a operazioni, risorse e condizioni

Quando configuri Controllo accessi e scrivi una politica di autorizzazioni da allegare a un'identità IAM (politiche basate sull'identità), puoi utilizzare gli elenchi di azioni, risorse e chiavi di condizione per Route 53, Azioni, risorse e chiavi di condizione per domini Route 53, azioni, risorse e chiavi di condizione per Route 53 Resolver, mentre Azioni, risorse e chiavi di condizione per Amazon Route 53 Profiles consente di condividere le impostazioni DNS nel Service Authorization Reference. VPCs Le pagine includono ogni azione dell'API Amazon Route 53, le azioni a cui devi concedere le autorizzazioni di accesso e la AWS risorsa a cui devi concedere l'accesso. Puoi specificare le azioni nel campo `Action` della policy e il valore della risorsa nel campo `Resource`.

Puoi utilizzare le chiavi di condizione AWS-wide nelle tue policy di Route 53 per esprimere condizioni. Per un elenco completo delle chiavi AWS-wide, consulta Available keys nella IAM User Guide.

> **Note**
>
> Quando si concede l'accesso, la zona ospitata e Amazon VPC devono appartenere alla stessa partizione. Una partizione è un gruppo di. Regioni AWS Ciascuno Account AWS è limitato a una partizione.
> Di seguito sono riportate le partizioni supportate:

- `aws` - Regioni AWS
- `aws-cn`: Regioni Cina
- `aws-us-gov` - AWS GovCloud (US) Region

Per ulteriori informazioni, consulta Gestione degli accessi in Riferimenti generali AWS .

> **Note**
>
> Per specificare un'operazione, utilizza il prefisso applicabile (`route53`, `route53domains` o `route53resolver`) seguito dal nome dell'operazione API, ad esempio:
>
> - `route53:CreateHostedZone`
> - `route53domains:RegisterDomain`
> - `route53resolver:CreateResolverEndpoint`

Registrazione e monitoraggio in Amazon Route 53

Amazon Route 53 offre la registrazione delle query DNS e la possibilità di monitorare le risorse utilizzando i controlli dell'integrità. Inoltre, Route 53 si integra con altri AWS servizi per fornire registrazione e monitoraggio aggiuntivi:

Registrazione di query DNS

È possibile configurare Route 53 per registrare le informazioni sulle query che Route 53 riceve, ad esempio il dominio o il sotto-dominio che è stato richiesto, la data e l'ora della richiesta e il tipo di record DNS, ad esempio A o AAAA.

Per ulteriori informazioni, consulta Registrazione delle query DNS pubbliche.

Utilizzo AWS CloudTrail per registrare le azioni programmatiche e della console

CloudTrail fornisce un registro delle azioni di Route 53 eseguite da un utente, un ruolo o un AWS servizio. Utilizzando le informazioni raccolte da CloudTrail, è possibile tenere traccia delle richieste effettuate, degli indirizzi IP da cui provengono le richieste, chi ha effettuato la richiesta, quando è stata effettuata e di ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon Route 53 con AWS CloudTrail.

Monitoraggio delle registrazioni di dominio

Il pannello di controllo di Route 53 fornisce informazioni dettagliate sullo stato delle registrazioni dei domini, ad esempio lo stato del trasferimento dei domini e i domini che si avvicinano alla data di scadenza.

Per ulteriori informazioni, consulta Monitoraggio delle registrazioni di dominio.

Usa i controlli sanitari di Route 53 e Amazon CloudWatch per monitorare le tue risorse

Puoi monitorare le tue risorse creando controlli sanitari Route 53, che raccolgono ed elaborano dati grezzi in metriche leggibili quasi in tempo reale. CloudWatch

Per ulteriori informazioni, consulta Monitoraggio delle risorse con i controlli sanitari di Amazon Route 53 e Amazon CloudWatch.

Utilizzo di Amazon CloudWatch per monitorare gli endpoint Route 53 Resolver

Puoi utilizzarlo CloudWatch per monitorare il numero di query DNS inoltrate dagli endpoint Resolver.

Per ulteriori informazioni, consulta Monitoraggio degli endpoint Route 53 Resolver con Amazon CloudWatch.

Usando AWS Trusted Advisor

Trusted Advisor si basa sulle migliori pratiche apprese servendo AWS i clienti. Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Tutti i AWS clienti hanno accesso a cinque Trusted Advisor controlli. I clienti con un piano di supporto Business o Enterprise possono visualizzare tutti i Trusted Advisor controlli.

Per ulteriori informazioni, consulta Trusted Advisor.

Convalida della conformità per Amazon Route 53

Revisori di terze parti valutano la sicurezza e la conformità di Amazon Route 53 nell'ambito di diversi programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta AWS Services in Scope by Compliance Program. Per informazioni generali, consulta Programmi di conformità di AWS.

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact.

La tua responsabilità di conformità durante l'utilizzo di Route 53 è determinata dalla riservatezza dei dati, dagli obiettivi dell'azienda e dalle leggi e normative applicabili. Se l'uso di Route 53 è soggetto alla conformità a standard come HIPAA, PCI o FedRAMP, fornisce risorse per aiutarti a: AWS

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sulla progettazione per la sicurezza HIPAA e la conformità: questo whitepaper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni conformi ai requisiti HIPAA.
- AWS Risorse per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in Amazon Route 53

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Route 53 suddivide le proprie funzionalità in un piano dati e di controllo. Come la maggior parte dei servizi AWS , Route 53 comprende un piano di controllo (control-plane) che consente le operazioni di gestione, ad esempio creare, aggiornare e rimuovere le risorse, e un piano dati che fornisce le funzionalità principali del servizio. Per ulteriori informazioni sui piani dati e di controllo in Route 53, consulta Nozioni sul piano di controllo e sul piano dati.

Route 53 è principalmente un servizio globale, ma le seguenti funzionalità supportano le regioni: AWS

- Se utilizzi Route 53 Resolver per configurare configurazioni ibride, crei endpoint nelle AWS regioni che preferisci e specifichi gli indirizzi IP in più zone di disponibilità. Per gli endpoint in uscita, è necessario creare regole nella stessa regione in cui è stato creato l'endpoint. Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.
- Puoi configurare i controlli di integrità di Route 53 per verificare lo stato delle risorse che crei in regioni specifiche, come le EC2 istanze Amazon e i sistemi di bilanciamento del carico Elastic Load Balancing.
- Quando si crea un controllo dell'integrità che monitora un endpoint, è possibile specificare le regioni in cui si desidera che Route 53 esegua i controlli dell'integrità.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Sicurezza dell'infrastruttura in Amazon Route 53

In quanto servizio gestito, Amazon Route 53 è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere a Route 53 attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Invio dei risultati dal firewall DNS di Route 53 Resolver al Security Hub

AWS Security Hubti offre una visione completa dello stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Security Hub raccoglie dati sulla sicurezza da tutti Account AWS i prodotti partner di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e identificare i problemi di sicurezza con la massima priorità. Servizi AWS

Integrando Route 53 Resolver DNS Firewall con Security Hub, puoi inviare i risultati da DNS Firewall a Security Hub. Security Hub include quindi tali risultati nell'analisi del livello di sicurezza dell'utente.

Indice

Come funzionano i risultati in Security Hub

In Security Hub, un risultato è una registrazione osservabile di un controllo di sicurezza o di un rilevamento relativo alla sicurezza. Alcuni risultati derivano da problemi rilevati da altri partner Servizi AWS o da terze parti. Security Hub dispone anche dei propri controlli di sicurezza che utilizza per rilevare problemi di sicurezza e generare risultati.

Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi dei risultati e visualizzare i dettagli di un risultato. Per informazioni, consulta Esame dei dettagli dei risultati e della cronologia delle ricerche in Security Hub nella Guida AWS Security Hub per l'utente. Puoi anche aggiornare automaticamente i risultati o inviarli a un'azione personalizzata. Per ulteriori informazioni, consulta Modificare automaticamente e intervenire sui risultati del Security Hub nella Guida per l'AWS Security Hub utente.

Tutti i risultati in Security Hub utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema di sicurezza, sulle risorse interessate e sullo stato attuale del risultato. Per ulteriori informazioni, consulta AWS Security Finding Format (ASFF) nella Guida per l'utente di AWS Security Hub .

DNS Firewall è uno di quelli Servizi AWS che invia i risultati a Security Hub.

Tipi di risultati inviati da DNS Firewall

DNS Firewall include le seguenti integrazioni:

- Elenchi di domini gestiti: risultati di sicurezza relativi alle query bloccate o segnalate per i domini associati agli elenchi di domini gestiti. AWS
- Elenchi di domini personalizzati: risultati di sicurezza relativi alle query bloccate o segnalate per i domini associati all'elenco di domini del cliente.
- DNS Firewall Advanced: risultati di sicurezza relativi alle query bloccate o segnalate da DNS Firewall Advanced.

Security Hub acquisisce i risultati di DNS Firewall nel AWS Security Finding Format (ASFF). In ASFF, il `Types` campo fornisce il tipo di esito. I risultati di DNS Firewall possono avere i seguenti valori per. `Types`

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Riprovare quando Security Hub non è disponibile

Se Security Hub non è disponibile, DNS Firewall riprova a inviare i risultati finché non vengono ricevuti.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

DNS Firewall aggiornerà i risultati esistenti se lo stesso risultato viene nuovamente osservato.

Risultato tipico di DNS Firewall

Security Hub inserisce i risultati del firewall DNS nel AWS Security Finding Format (ASFF).

Ecco un esempio di un risultato tipico di DNS Firewall in ASFF.


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "00000000-0000-0000-0000-example1",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-
resolver-dns-firewall-aws-list",
            "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
            "CompanyName": "Amazon",
            "Region": "us-east-1",
            "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-
rule-group/rslvr-frg-example1",
            "AwsAccountId": "000000000000",
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ],
            "FirstObservedAt": "2024-12-06T19:58:49.000Z",
            "LastObservedAt": "2024-12-06T19:58:49.000Z",
            "CreatedAt": "2024-12-06T19:58:49.000Z",
            "UpdatedAt": "2024-12-06T19:58:49.000Z",
            "Severity": {
                "Label": "HIGH",
                "Normalized": 70
            },
            "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC
 vpc-example1",
            "Description": "DNS Firewall ALERT",
            "ProductFields": {
                "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
                "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-
example1",
                "aws/route53resolver/dnsfirewall/queryType": "A",
                "aws/route53resolver/dnsfirewall/queryClass": "IN",
                "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-
example1",
                "aws/route53resolver/dnsfirewall/transport": "UDP",
                "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
                "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
 List",
                "aws/securityhub/CompanyName": "Amazon"
            },
            "Resources": [
```

```
                {
                    "Type": "Other",
                    "Id": "rslvr-in-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "ResourceType": "ResolverEndpoint",
                            "EndpointId": "rslvr-in-example1"
                        }
                    }
                },
                {
                    "Type": "Other",
                    "Id": "rni-example1",
                    "Partition": "aws",
                    "Region": "us-east-1",
                    "Details": {
                        "Other": {
                            "NetworkInterfaceId": "rni-example1",
                            "ResourceType": "ResolverNetworkInterface"
                        }
                    }
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "HIGH"
                },
                "Types": [
                    "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
                ]
            },
            "ProcessedAt": "2024-12-11T19:33:35.494Z"
        }
```

Abilitazione e configurazione dell'integrazione

Per integrare DNS Firewall con Security Hub, devi prima abilitare Security Hub. Per informazioni sull'attivazione di Security Hub, vedere Enabling Security Hub nella Guida AWS Security Hub per l'utente.

Interruzione dell'invio dei risultati a Security Hub

Per interrompere l'invio dei risultati del firewall DNS a Security Hub, puoi utilizzare la console Security Hub o l'API Security Hub.

Per istruzioni, consulta Disabilitazione del flusso di risultati da un'integrazione nella Guida per l'AWS Security Hub utente.

Monitoraggio di Amazon Route 53

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle soluzioni. AWS È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Tuttavia, prima di iniziare il monitoraggio è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Argomenti

Registrazione delle query DNS pubbliche

Puoi configurare Amazon Route 53 per registrare le informazioni sulle query DNS pubbliche ricevute da Amazon Route 53, ad esempio le seguenti:

- Dominio o sottodominio richiesto

- Data e ora della richiesta
- Tipo di record DNS (ad esempio A o AAAA)
- Edge location Route 53 che ha risposto alla query DNS
- Codice di risposta DNS, ad esempio `NoError` o `ServFail`

Una volta configurata la registrazione delle interrogazioni, Route 53 invierà i log a Logs. CloudWatch Si utilizzano gli strumenti CloudWatch Logs per accedere ai log delle interrogazioni.

I log di query contengono solo le query che i resolver DNS inoltrano a Route 53. Se un resolver DNS ha già memorizzato nella cache la risposta a una query (ad esempio l'indirizzo IP per un load balancer per esempio.com), il resolver continuerà a restituire la risposta memorizzata nella cache senza inoltrare le query a Route 53 finché il TTL per il record corrispondente non scade.

In base al numero di query DNS inviate per un nome di dominio (esempio.com) o di sottodominio (www.esempio.com), che gli utenti usano, e in base al TTL per il record, i log delle query potrebbero contenere informazioni su una sola query su diverse migliaia di query che vengono inviate ai resolver DNS. Per ulteriori informazioni sul funzionamento di DNS, consulta In che modo il traffico Internet viene instradato al tuo sito o applicazione Web.

Se non hai bisogno di informazioni di registrazione dettagliate, puoi utilizzare i CloudWatch parametri di Amazon per vedere il numero totale di query DNS a cui Route 53 risponde per una zona ospitata. Per ulteriori informazioni, consulta Visualizzazione dei parametri delle query DNS per una zone ospitata pubblica.

Argomenti

Configurare la registrazione per le query DNS

Per avviare la registrazione delle query DNS per una determinata zona ospitata, puoi eseguire le seguenti attività nella console Amazon Route 53:

- Scegli il gruppo di log CloudWatch Logs in cui desideri che Route 53 pubblichi i log o crea un nuovo gruppo di log.

> **Note**
>
> Il gruppo di log deve trovarsi nella regione Stati Uniti orientali (Virginia settentrionale).

- Scegli Create (Crea policy) per terminare.

> **Note**
>
> Se gli utenti inviano query DNS per il tuo dominio, dovresti iniziare a visualizzare le query nei registri nel giro di pochi minuti dopo aver creato la configurazione di registrazione delle query.

Per configurare la registrazione per le query DNS

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli la zona ospitata per cui configurare la registrazione delle query.
4. Nel riquadro Hosted zone details (Dettagli zona ospitata), seleziona Configure query logging (Configura registrazione query).
5. Scegli un gruppo di log esistente o creane uno nuovo.
6. Se viene visualizzato un avviso relativo alle autorizzazioni (nel caso in cui non è stata configurata la registrazione delle query con la nuova console in precedenza), completare una delle operazioni seguenti:
   - Se disponi già di 10 policy delle risorse, non sarà possibile crearne altre. Seleziona una delle policy delle risorse e seleziona Modifica. La modifica darà a Route 53 le autorizzazioni per scrivere i log nei gruppi di log. Seleziona Salva. L'avviso scomparirà e sarà possibile continuare con la fase successiva.
   - Se non hai mai configurato la registrazione delle query in precedenza (o se non hai già creato 10 policy relative alle risorse), devi concedere le autorizzazioni a Route 53 per scrivere i log nei tuoi CloudWatch gruppi Logs. Scegli Concedi autorizzazioni. L'avviso scomparirà e sarà possibile continuare con la fase successiva.

7. Scegli Autorizzazioni: facoltativo per visualizzare una tabella che mostra se la politica delle risorse corrisponde al gruppo di CloudWatch log e se Route 53 dispone dell'autorizzazione per pubblicare i log. CloudWatch
8. Scegli Create (Crea) .

Utilizzo di Amazon CloudWatch per accedere ai log delle query DNS

Amazon Route 53 invia i log delle query direttamente a CloudWatch Logs; i log non sono mai accessibili tramite Route 53. Utilizza invece CloudWatch Logs per visualizzare i log quasi in tempo reale, cercare e filtrare i dati ed esportare i log su Amazon S3.

Route 53 crea un flusso di log di CloudWatch Logs per ogni edge location di Route 53 che risponde alle query DNS per la zona ospitata specificata e invia i log delle query al flusso di log applicabile. Il formato per il nome di ogni flusso di log è*hosted-zone-id*/*edge-location-ID*, ad esempio,. `Z1D633PJN98FT9/DFW3`

Ogni posizione del bordo è identificata da un codice di tre lettere e da un numero assegnato arbitrariamente, ad esempio. DFW3 Il codice di tre lettere di solito corrisponde al codice aeroportuale della International Air Transport Association per l'aeroporto vicino alla edge location. (Queste abbreviazioni potrebbero cambiare in futuro). Per un elenco di edge location, consulta "La rete globale di Route 53" nella pagina dei dettagli di prodotto di Route 53.

> **Note**
>
> È possibile che vengano visualizzati alcuni prefissi o suffissi che non seguono la convenzione di cui sopra. Questi attributi codificano solo per uso interno.

Per ulteriori informazioni, consulta la documentazione relativa:

- Guida per l'utente CloudWatch di Amazon Logs
- Riferimento all'API Amazon CloudWatch Logs
- CloudWatch Sezione Logs del Command Reference AWS CLI
- Valori che vengono visualizzati nei log di query DNS

Modifica del periodo di conservazione per i log ed esportazione dei log su Amazon S3

Per impostazione predefinita, CloudWatch Logs archivia i log delle interrogazioni a tempo indeterminato. Facoltativamente, è possibile specificare un periodo di conservazione in modo che CloudWatch Logs elimini i log più vecchi del periodo di conservazione. Per ulteriori informazioni, consulta Change log data retention in CloudWatch Logs nella Amazon CloudWatch User Guide.

Se desideri conservare i dati di log ma non hai bisogno degli strumenti CloudWatch Logs per visualizzare e analizzare i dati, puoi esportare i log su Amazon S3, in modo da ridurre i costi di storage. Per ulteriori informazioni, consulta Esportazione di dati di log su Amazon S3.

Per informazioni sui prezzi, consulta la pagina relativa:

- «Amazon CloudWatch Logs» nella pagina dei CloudWatch prezzi
- Prezzi di Amazon S3

> **Note**
>
> Quando configuri Route 53 per registrare query DNS non ti sarà addebitato alcun costo per Route 53.

Arresto della registrazione di query

Se desideri che Amazon Route 53 interrompa l'invio dei log delle query a CloudWatch Logs, esegui la seguente procedura per eliminare la configurazione di registrazione delle query.

Eliminare una configurazione di registrazione delle query

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel pannello di navigazione, scegli Zone ospitate.
3. Scegli il nome per la zona ospitata per cui desideri eliminare la configurazione di registrazione delle query.
4. Nel riquadro Dettagli zona ospitata, seleziona Elimina configurazione di registrazione delle query.
5. Seleziona Elimina per confermare.

Valori che vengono visualizzati nei log di query DNS

Ogni file di log contiene una voce di log per ogni query DNS che Amazon Route 53 ha ricevuto dai resolver DNS nella posizione edge corrispondente. Ogni voce di log include i seguenti valori:

Tipo di formato del log

Il numero di versione di questo log di query. Se aggiungiamo campi al log o modifichiamo il formato dei campi esistenti, incrementeremo questo valore.

Timestamp di query

La data e l'ora in cui Route 53 ha risposto alla richiesta, in formato ISO 8601 e UTC, ad esempio `2017-03-16T19:20:25.177Z`.

Per informazioni sul formato ISO 8601, consulta l'articolo di Wikipedia ISO 8601. Per informazioni su UTC, consulta l'articolo di Wikipedia Coordinated Universal Time.

ID della hosted zone

L'ID della zona ospitata che è associata a tutte le query DNS in questo record.

Nome query

Il dominio o sottodominio specificato nella richiesta.

Tipo di query

Il tipo di record DNS specificato nella richiesta, o `ANY`. Per ulteriori informazioni sui tipi supportati da Route 53, consulta Tipi di record DNS supportati.

Codice di risposta

Il codice di risposta DNS che Route 53 ha restituito in risposta alla query DNS.

Protocollo di livello 4

Il protocollo che è stato usato per inviare la query, `TCP` o `UDP`.

Posizione edge di Route 53

La posizione edge di Route 53 che ha risposto alla query. Ogni edge location è identificata, ad esempio, da un codice di tre lettere e da un numero arbitrario. DFW3 Il codice di tre lettere di solito corrisponde al codice aeroportuale della International Air Transport Association per l'aeroporto vicino alla edge location. (Queste abbreviazioni potrebbero cambiare in futuro).

Per un elenco di posizioni edge, consulta "La rete globale di Route 53" nella pagina Dettagli di prodotto di Route 53.

Indirizzo IP del resolver

L'indirizzo IP del resolver DNS che ha inviato la richiesta a Route 53.

Sottorete client EDNS

Un indirizzo IP parziale per il client da cui la richiesta ha avuto origine, se disponibile dal resolver DNS.

Per ulteriori informazioni, consulta la bozza IETF Client Subnet in DNS Requests.

Esempio di log di query

Ecco un esempio di registro di query (la Regione è un placehoeder):

```
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 -
```

Registrazione delle query di Resolver

È possibile registrare le seguenti query DNS:

- Query che hanno origine in Amazon Virtual Private Cloud VPCs da te specificate, nonché le risposte a tali query DNS.
- Query da risorse on-premise che utilizzano un endpoint Resolver in ingresso.
- Query che utilizzano un endpoint Resolver in uscita per la risoluzione DNS ricorsiva.
- Query che utilizzano le regole di DNS Firewall per Route 53 Resolver per bloccare, consentire o monitorare gli elenchi di dominio.

I log delle query di Resolver includono valori come i seguenti:

- La AWS regione in cui è stato creato il VPC
- L'ID dell'VPC da cui è stata originata la query
- L'indirizzo IP dell'istanza da cui è stata originata la query
- L'ID istanza della risorsa da cui è stata originata la query
- La data e l'ora in cui la query è stata eseguita per la prima volta
- Il nome DNS richiesto (ad esempio prod.esempio.com)
- Il tipo di record DNS (ad esempio A o AAAA)
- Il codice di risposta DNS, ad esempio `NoError` o `ServFail`
- I dati di risposta DNS, ad esempio l'indirizzo IP che viene restituito in risposta alla query DNS
- Una risposta a un'operazione della regola DNS Firewall

Per un elenco dettagliato di tutti i valori registrati e un esempio, consulta Valori che vengono visualizzati nei log di query di Resolver.

> **Note**
>
> Come di norma per i resolver DNS, i resolver memorizzano nella cache le query DNS per un periodo di tempo determinato dal (TTL) del resolver. time-to-live Il Route 53 Resolver memorizza nella cache le query che hanno origine nell'utente e risponde dalla cache ogni volta che è possibile per velocizzare le risposte. VPCs La registrazione delle query del resolver registra solo le query univoche, non le query a cui Resolver è in grado di rispondere dalla cache.
>
> Ad esempio, supponiamo che un' EC2 istanza in una delle configurazioni per cui una configurazione di registrazione delle query sta registrando le VPCs query, invii una richiesta a accounting.example.com. Resolver memorizza nella cache la risposta a tale query e registra la query. Se l'interfaccia di rete elastica della stessa istanza esegue una query per accounting.esempio.com all'interno del TTL della cache di Resolver, Resolver risponde alla query dalla cache. La seconda query non viene registrata.

È possibile inviare i log a una delle seguenti risorse: AWS

- Gruppo di CloudWatch log Amazon Logs (CloudWatch Logs)

- Bucket di Amazon S3 (S3)
- Flussi di distribuzione Firehose

Per ulteriori informazioni, consulta AWS risorse a cui puoi inviare i log delle query di Resolver.

Argomenti

AWS risorse a cui puoi inviare i log delle query di Resolver

> **Note**
>
> Se prevedi di registrare le query per carichi di lavoro con query elevate al secondo (QPS), è consigliabile utilizzare Amazon S3 per garantire che i log delle query non siano limitati quando vengono scritti sulla destinazione. Se utilizzi Amazon CloudWatch, puoi aumentare il limite di richieste al secondo per l'`PutLogEvents`operazione. Per ulteriori informazioni sull'aumento CloudWatch dei limiti, consulta CloudWatch Logs quotas nella Amazon CloudWatch User Guide.

Puoi inviare i log delle query di Resolver alle seguenti risorse: AWS

Gruppo di CloudWatch log Amazon Logs (Amazon CloudWatch Logs)

Puoi analizzare i log con Logs Insights e creare parametri e allarmi.

Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

Bucket di Amazon S3 (S3)

Un bucket S3 è una opzione economica per l'archiviazione dei log a lungo termine. La latenza è in genere superiore.

Tutte le opzioni di crittografia lato server S3 sono supportate. Per ulteriori informazioni, consulta Protezione dei dati con la crittografia lato server nella Guida per l'utente di Amazon S3.

Se il bucket S3 si trova in un account di tua proprietà, le autorizzazioni richieste vengono automaticamente aggiunte alla tua policy relativa ai bucket. Se desideri inviare i log a un bucket

S3 in un account di cui non si è proprietari, il proprietario del bucket S3 deve aggiungere le autorizzazioni per l'account nelle policy del bucket. Ad esempio:

```
{
    "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**
>
> Se desideri archiviare i log in un bucket S3 centrale per l'organizzazione, è consigliabile impostare la configurazione della registrazione delle query da un account centralizzato (con le autorizzazioni necessarie per scrivere in un bucket centrale) e utilizzare RAM per condividere la configurazione tra gli account.

Per ulteriori informazioni, consultare la Guida per l'utente di Amazon Simple archiviazione Service.

Flussi di distribuzione Firehose

Puoi trasmettere i log in tempo reale su Amazon OpenSearch Service, Amazon Redshift o altre applicazioni.

Per ulteriori informazioni, consulta la Amazon Data Firehose Developer Guide.

Per informazioni sui prezzi per la registrazione delle query con Resolver, consulta i prezzi di Amazon. CloudWatch

CloudWatch I costi di Vented Logs si applicano quando si utilizzano i log Resolver, anche quando i log vengono pubblicati direttamente su Amazon S3. Per ulteriori informazioni, consulta la pagina dei prezzi di Logs nella pagina dei prezzi di Amazon CloudWatch .

Gestione delle configurazioni di registrazione delle query di Resolver

Configurazione (registrazione delle query di Resolver)

Per iniziare a registrare le query DNS che hanno origine nel tuo VPCs, esegui le seguenti attività nella console Amazon Route 53:

Come configurare la registrazione delle query di Resolver

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Espandi il menu della console Route 53. Nell'angolo in alto a sinistra della console, scegli l'icona con le tre barre orizzontali (☰).
3. Nel menu Resolver, scegli Registrazione delle query.
4. Nel selettore Regione, scegli la AWS regione in cui desideri creare la configurazione di registrazione delle interrogazioni. Questa deve essere la stessa regione in cui hai creato la regione per VPCs cui desideri registrare le query DNS. Se ti trovi VPCs in più regioni, devi creare almeno una configurazione di registrazione delle query per ogni regione.
5. Scegli Configura registrazione delle query.
6. Specifica i seguenti valori:

Nome della configurazione della registrazione delle query

Specifica un nome per la configurazione della registrazione delle query. Il nome sarà visualizzato nella console nell'elenco delle configurazioni di registrazione delle query. Specifica un nome che consenta di trovare facilmente questa configurazione in un secondo momento.

Destinazione dei log delle query

Scegli il tipo di AWS risorsa a cui desideri che Resolver invii i log delle query. Per informazioni su come scegliere tra le opzioni (CloudWatch Logs log group, S3 bucket e Firehose delivery stream), consulta. AWS risorse a cui puoi inviare i log delle query di Resolver

Dopo aver scelto il tipo di risorsa, puoi creare un'altra risorsa di quel tipo o scegliere una risorsa esistente creata dall'account corrente. AWS

> **Note**
>
> È possibile scegliere solo le risorse create nella AWS regione scelta nel passaggio 4, la regione in cui si sta creando la configurazione di registrazione delle query. Se decidi di creare una nuova risorsa, tale risorsa verrà creata nella stessa regione.

VPCs per registrare le interrogazioni per

Questa configurazione di registrazione delle query registrerà le query DNS che hanno origine nel server scelto dall' VPCs utente. Seleziona la casella di controllo relativa a ciascun VPC nella regione corrente per cui desideri che il Resolver record le query, quindi seleziona Scegli.

> **Note**
>
> La consegna dei log VPC può essere abilitata una sola volta per un tipo di destinazione specifico. I log non possono essere consegnati a più destinazioni dello stesso tipo, ad esempio, i log VPC non possono essere consegnati a 2 destinazioni Amazon S3.

7. Scegli Configura registrazione delle query.

> **Note**
>
> Le query DNS eseguite dalle risorse nel VPC vengono visualizzate nei log dopo pochi minuti dalla creazione della configurazione della registrazione delle query.

Valori che vengono visualizzati nei log di query di Resolver

Ogni file di log contiene una voce di log per ogni query DNS che Amazon Route 53 ha ricevuto dai resolver DNS nella posizione edge corrispondente. Ogni voce di log include i seguenti valori:

version

Il numero di versione del formato del log di query. La versione corrente è `1.1`.

Il valore della versione è una versione principale e secondaria nel formato **`major_version.minor_version`**. Ad esempio, puoi avere un valore `version` di `1.7`, dove 1 è la versione principale e 7 è la versione secondaria.

Route 53 incrementa la versione principale se viene apportata una modifica alla struttura dei log che non è compatibile con le versioni precedenti. Questo include la rimozione di un campo JSON che esiste già o la modifica del modo in cui i contenuti di un campo sono rappresentati (ad esempio, un formato di data).

Route 53 incrementa la versione secondaria se una modifica aggiunge nuovi campi al file di log. Ciò può verificarsi se sono disponibili nuove informazioni per alcune o tutte le query DNS esistenti all'interno di un VPC.

account_id

L'ID dell' AWS account che ha creato il VPC.

Regione

La AWS regione in cui hai creato il VPC.

vpc_id

L'ID del VPC in cui è stata originata la query.

query_timestamp

La data e l'ora in cui la query è stata inoltrata, in formato ISO 8601 e UTC, ad esempio `2017-03-16T19:20:177Z`.

Per informazioni sul formato ISO 8601, consulta l'articolo di Wikipedia ISO 8601. Per informazioni su UTC, consulta l'articolo di Wikipedia Coordinated Universal Time.

query_name

Il nome di dominio (esempio.com) o di sottodominio (www.esempio.com) specificato nella query.

query_type

Il tipo di record DNS specificato nella richiesta, o `ANY`. Per ulteriori informazioni sui tipi supportati da Route 53, consulta Tipi di record DNS supportati.

query_class

La classe della query.

rcode

Il codice di risposta DNS che Resolver ha restituito in risposta alla query DNS. Il codice di risposta indica se la query era valida o meno. Il codice di risposta più comune è `NOERROR`, che indica che la query era valida. Se la risposta non è valida, Resolver restituisce un codice di risposta che spiega il motivo. Per un elenco dei possibili codici di risposta, consulta DNS RCODEs sul sito Web IANA.

answer_type

Il tipo di record DNS (ad esempio A, MX o CNAME) del valore restituito da Resolver in risposta alla query. Per ulteriori informazioni sui tipi supportati da Route 53, consulta Tipi di record DNS supportati.

rdata

Il valore restituito da Resolver in risposta alla query. Ad esempio, per un record A, si tratta di un indirizzo IP in IPv4 formato. Per un record CNAME, questo è il nome di dominio nel record CNAME.

answer_class

La classe della risposta del Resolver alla query.

srcaddr

L'indirizzo IP dell'istanza da cui è stata originata la query.

srcport

La porta dell'istanza da cui è stata originata la query.

Trasporto

Il protocollo utilizzato per inviare la query DNS.

srcids

IDs del`instance`,`resolver_endpoint`, e `resolver_network_interface` quello da cui è stata originata o trasmessa la query DNS.

istanza

L'ID dell'istanza in cui è stata originata la query.

> **Note**
>
> Se vedi un ID di istanza nei log delle Amazon Route 53 Resolver query che non è visibile nel tuo account, è possibile che la query DNS provenga da AWS Lambda Amazon EKS o dalla console Fargate AWS CloudShell, che è stata utilizzata da te.

resolver_endpoint

L'ID dell'endpoint del resolver che passa la query DNS ai server DNS on-premise.

firewall_rule_group_id

L'ID del gruppo di regole di DNS Firewall che corrisponde al nome di dominio nella query. Questa operazione viene compilata solo se DNS Firewall ha trovato una corrispondenza per una regola con azione impostata per l'avviso o il blocco.

Per ulteriori informazioni sui gruppi di regole del firewall, consulta Gruppi di regole e regole in DNS Firewall.

firewall_rule_action

L'operazione specificata dalla regola che corrisponde al nome di dominio nella query. Questa operazione viene compilata solo se DNS Firewall ha trovato una corrispondenza per una regola con azione impostata per l'avviso o il blocco.

firewall_domain_list_id

L'elenco di domini utilizzato dalla regola che corrisponde al nome di dominio nella query. Questa operazione viene compilata solo se DNS Firewall ha trovato una corrispondenza per una regola con azione impostata per l'avviso o il blocco.

proprietà_aggiuntive

Informazioni aggiuntive sugli eventi di consegna dei log. is_delayed: se c'è un ritardo nella consegna dei log.

Esempio di log delle query di Route 53 Resolver

Ecco un esempio di log delle query del resolver:

```
    {
      "srcaddr": "4.5.64.102",
      "vpc_id": "vpc-7example",
      "answers": [
          {
              "Rdata": "203.0.113.9",
              "Type": "PTR",
              "Class": "IN"
          }
      ],
      "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
      "firewall_rule_action": "BLOCK",
      "query_name": "15.3.4.32.in-addr.arpa.",
      "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
      "query_class": "IN",
      "srcids": {
          "instance": "i-0d15cd0d3example"
      },
      "rcode": "NOERROR",
      "query_type": "PTR",
      "transport": "UDP",
      "version": "1.100000",
      "account_id": "111122223333",
      "srcport": "56067",
      "query_timestamp": "2021-02-04T17:51:55Z",
      "region": "us-east-1"
  }
```

Condivisione delle configurazioni di registrazione delle query di Resolver con altri account AWS

È possibile condividere le configurazioni di registrazione delle interrogazioni create utilizzando un account con altri account. AWS AWS Per condividere le configurazioni, la console Route 53 Resolver

si integra con Resource Access Manager AWS . Per ulteriori informazioni su Resource Access Manager, consulta la Guida per l'utente a Resource Access Manager.

Tieni presente quanto segue:

Associazione a configurazioni di registrazione delle VPCs query condivise

Se un altro AWS account ha condiviso una o più configurazioni con il tuo account, puoi associarlo alla VPCs configurazione nello stesso modo in cui lo fai VPCs con le configurazioni che hai creato.

Eliminazione o annullamento di una condivisione di una configurazione

Se condividi una configurazione con altri account e poi elimini la configurazione o interrompi la condivisione e se uno o più VPCs sono associati alla configurazione, Route 53 Resolver interrompe la registrazione delle query DNS che provengono da tali account. VPCs

Numero massimo di configurazioni di registrazione delle query, che possono essere associate a una configurazione VPCs

Quando un account crea una configurazione e la condivide con uno o più altri account, viene applicato il numero massimo di configurazioni VPCs che è possibile associare alla configurazione per account. Ad esempio, se l'organizzazione dispone di 10.000 account, è possibile creare la configurazione di registrazione delle query nell'account centrale e condividerla tramite AWS RAM per condividerla con gli account dell'organizzazione. Gli account dell'organizzazione assoceranno quindi la configurazione al loro VPCs conteggio rispetto alla configurazione del registro di query dell'account (associazioni VPC) Regione AWS per limite di 100. Tuttavia, se tutti si VPCs trovano in un unico account, potrebbe essere necessario aumentare i limiti di servizio dell'account.

Per le quote correnti di Resolver, consulta Quote relative a Route 53 Resolver.

Autorizzazioni

Per condividere una regola con un altro AWS account, devi disporre dell'autorizzazione per utilizzare l'PutResolverQueryLogConfigPolicyazione.

Restrizioni sull' AWS account con cui è condivisa una regola

L'account con cui si condivide una regola non può modificare né eliminare la regola.

Assegnazione di tag

Solo l'account che ha creato una regola può aggiungere, eliminare o visualizzare i tag della regola.

Per visualizzare lo stato di condivisione corrente di una regola (incluso l'account che ha condiviso la regola o l'account con cui la regola è condivisa) e per condividere regole con un altro account, procedi nel seguente modo.

Come visualizzare lo stato di condivisione e le configurazioni di registrazione delle query condivise con un altro account AWS

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegliere Registrazione delle query.
3. Nella barra di navigazione, selezionare la regione dove è stata creata la regola.

   La colonna Sharing status (Stato condivisione) mostra l'attuale stato delle regole create dall'account attuale o condivise con l'account attuale.

   - Non condivisa: l' AWS account corrente ha creato la regola e la regola non è condivisa con altri account.
   - Condivisa da me: l'attuale account ha creato la regola e l'ha condivisa con uno o più account.
   - Condivisa con me: un altro account ha creato la regola e l'ha condivisa con l'account attuale.
4. Scegliere il nome della regola di cui si desidera visualizzare le informazioni di condivisione o che si desidera condividere con un altro account.

   Nella *rule name* pagina Regola:, il valore in Proprietario mostra l'ID dell'account che ha creato la regola. Questo è l'account attuale, a meno che il valore di Sharing status (Stato di condivisione) non sia Shared with me (Condivisa con me). In questo caso, il Owner (Proprietario) è l'account che ha creato la regola e l'ha condivisa con l'account attuale.

   Viene visualizzato anche lo stato della condivisione.
5. Scegli Condividi configurazione per aprire la AWS RAM console
6. Per creare una condivisione di risorse, segui i passaggi descritti in Creazione di una condivisione di risorse AWS RAM nella guida per l'AWS RAM utente.

> **Note**
>
> Non è possibile aggiornare le impostazioni di condivisione. Se vuoi modificare una delle seguenti impostazioni, devi ricondividere una regola con le nuove impostazioni e rimuovere le precedenti impostazioni di condivisione.

Monitoraggio delle registrazioni di dominio

Il pannello di controllo di Amazon Route 53 fornisce informazioni dettagliate sullo stato delle registrazioni di dominio, tra cui:

- Status delle nuove registrazioni di dominio
- Stato dei trasferimenti di dominio a Route 53
- Elenco dei domini che si avvicinano alla data di scadenza

Ti consigliamo di verificare periodicamente il pannello di controllo della console Route 53, soprattutto dopo la registrazione di un nuovo dominio o il trasferimento di un dominio a Route 53, per confermare che non ci siano problemi da affrontare.

Ti consigliamo inoltre di verificare che i dati di contatto per i tuoi domini siano aggiornati. Poiché la data di scadenza per un dominio si avvicina, inviamo un'e-mail al contatto del registrant per il dominio con informazioni su quando il dominio scade e su come effettuare il rinnovo.

Monitoraggio delle risorse con i controlli sanitari di Amazon Route 53 e Amazon CloudWatch

Puoi monitorare le tue risorse creando controlli di integrità di Amazon Route 53, che vengono utilizzati CloudWatch per raccogliere ed elaborare dati grezzi in metriche leggibili quasi in tempo reale. Queste statistiche vengono registrate per un periodo di due settimane, per permettere l'accesso a informazioni storiche e per offrire una prospettiva migliore sulle prestazioni delle risorse. Per impostazione predefinita, i dati metrici per i controlli sanitari di Route 53 vengono inviati automaticamente a CloudWatch intervalli di un minuto.

Per altre informazioni sui controlli dell'integrità di Route 53, consulta Monitoraggio dei controlli sanitari tramite CloudWatch. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

Parametri e dimensioni per i controlli dell'integrità di Route 53

Quando crei un controllo dello stato, Amazon Route 53 inizia a inviare parametri e dimensioni una volta al minuto alla CloudWatch risorsa specificata. La console Route 53 consente di visualizzare lo stato dei controlli dell'integrità. Puoi anche utilizzare le seguenti procedure per visualizzare i parametri nella CloudWatch console o visualizzarli utilizzando AWS Command Line Interface ()AWS CLI.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Nella scheda All metrics (Tutti i parametri) scegliere Route 53.
4. Scegliere Health Check Metrics (Parametri di controllo dell'integrità).

Per visualizzare le metriche utilizzando il AWS CLI

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Argomenti

- CloudWatch metriche per i controlli sanitari di Route 53
- Dimensioni per i parametri dei controlli dell'integrità di Route 53

CloudWatch metriche per i controlli sanitari di Route 53

Lo spazio dei nomi `AWS/Route53` include i seguenti parametri per i controlli dell'integrità di Route 53.

ChildHealthCheckHealthyCount

Per un controllo dell'integrità calcolato, il numero di controlli di integrità sani.

Statistiche valide: Average ((consigliata), Minimum, Maximum

Unità: numero

ConnectionTime

Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per stabilire una connessione TCP con l'endpoint. Puoi visualizzare `ConnectionTime` per un controllo dell'integrità per tutte le regioni o per una regione geografica selezionata.

Statistiche valide: Average ((consigliata), Minimum, Maximum

Unità: millisecondi

HealthCheckPercentageHealthy

La percentuale di strumenti di controllo dell'integrità di Route 53 che considera l'endpoint selezionato come integro.

Statistiche valide: Average (Media), Minimum, Maximum

Unità: percentuale

HealthCheckStatus

Lo stato dell'endpoint di controllo dello stato di salute che CloudWatch sta controllando. 1 indica uno stato di salute e 0 indica uno stato di salute non corretto.

Statistiche valide: minimo, medio e massimo

Unità: nessuna

SSLHandshakeOra

Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per completare l'handshake SSL. Puoi visualizzare `SSLHandshakeTime` per un controllo dell'integrità per tutte le regioni o per una regione geografica selezionata.

Statistiche valide: Average ((consigliata), Minimum, Maximum

Unità: millisecondi

TimeToFirstByte

Il tempo medio, in millisecondi, che è servito agli strumenti di controllo dell'integrità di Route 53 per ricevere il primo byte della risposta a una richiesta HTTP o HTTPS. Puoi visualizzare `TimeToFirstByte` per un controllo dell'integrità per tutte le regioni o per una regione geografica selezionata.

Statistiche valide: Average ((consigliata), Minimum, Maximum

Unità: millisecondi

Dimensioni per i parametri dei controlli dell'integrità di Route 53

I parametri di Route 53 per i controlli dell'integrità utilizzano lo spazio dei nomi `AWS/Route53` e forniscono i parametri per `HealthCheckId`. Quando recuperi i parametri, devi fornire la dimensione `HealthCheckId`.

Inoltre, per `ConnectionTime`, `SSLHandshakeTime` e `TimeToFirstByte`, puoi specificare in via opzionale `Region`. Se omettiRegion, CloudWatch restituisce le metriche in tutte le regioni. Se includiRegion, CloudWatch restituisce le metriche solo per la regione specificata.

Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

Monitoraggio delle zone ospitate tramite Amazon CloudWatch

Puoi monitorare le tue zone pubbliche ospitate utilizzando Amazon CloudWatch per raccogliere ed elaborare dati grezzi in metriche leggibili quasi in tempo reale. Le metriche sono disponibili poco dopo che Route 53 riceve le query DNS su cui si basano le metriche. CloudWatch i dati metrici per le zone ospitate di Route 53 hanno una granularità di un minuto.

Per ulteriori informazioni, consulta la seguente documentazione

- Per una panoramica e informazioni su come visualizzare le metriche nella CloudWatch console Amazon e su come recuperare le metriche utilizzando AWS Command Line Interface ()AWS CLI, consulta Visualizzazione dei parametri delle query DNS per una zone ospitata pubblica
- Per informazioni sul periodo di conservazione delle metriche, consulta GetMetricStatisticsAmazon CloudWatch API Reference.
- Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.
- Per ulteriori informazioni sui CloudWatch parametri, consulta Using Amazon CloudWatch metrics nella Amazon CloudWatch User Guide.

Argomenti

- CloudWatch metriche per le zone ospitate pubbliche di Route 53
- CloudWatch dimensione per le metriche delle zone ospitate pubbliche di Route 53

CloudWatch metriche per le zone ospitate pubbliche di Route 53

Lo spazio dei nomi `AWS/Route53` include i seguenti parametri per le zone ospitate di Route 53:

DNSQueries

Per una zona ospitata, il numero di query DNS a cui Route 53 risponde in un periodo di tempo specificato.

Statistiche valide: somma, SampleCount

Unità: numero

Regione: Route 53 è un servizio globale. Per ottenere i parametri delle zone ospitate, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione.

DNSSECInternalFallimento

Il valore è 1 se un qualsiasi oggetto nella zona ospitata si trova nello stato INTERNAL_FAILURE. In caso contrario, il valore è 0.

Statistiche valide: somma

Unità: numero

Volume: 1 per 4 ore per zona ospitata

Regione: Route 53 è un servizio globale. Per ottenere i parametri delle zone ospitate, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione.

DNSSECKeySigningKeysNeedingAction

Numero di chiavi per la firma delle chiavi (KSKs) con stato ACTION_NEEDED (a causa di un errore KMS).

Statistiche valide: somma, SampleCount

Unità: numero

Volume: 1 per 4 ore per zona ospitata

Regione: Route 53 è un servizio globale. Per ottenere i parametri delle zone ospitate, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione.

DNSSECKeySigningKeyMaxNeedingActionAge

Tempo trascorso da quando la chiave di firma delle chiavi (KSK) è stata impostata sullo stato ACTION_NEEDED.

Statistiche valide: massimo

Unità: secondi

Volume: 1 per 4 ore per zona ospitata

Regione: Route 53 è un servizio globale. Per ottenere i parametri delle zone ospitate, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione.

DNSSECKeySigningKeyAge

Tempo trascorso dalla creazione della chiave di firma delle chiavi (KSK) (non da quando è stata attivata).

Statistiche valide: massimo

Unità: secondi

Volume: 1 per 4 ore per zona ospitata

Regione: Route 53 è un servizio globale. Per ottenere i parametri delle zone ospitate, occorre specificare Stati Uniti orientali (Virginia settentrionale) per la regione.

CloudWatch dimensione per le metriche delle zone ospitate pubbliche di Route 53

I parametri di Route 53 delle zone ospitate utilizzano lo spazio dei nomi `AWS/Route53` e forniscono i parametri per `HostedZoneId`. Per ottenere il numero di query DNS, occorre specificare l'ID della zona ospitata nella dimensione `HostedZoneId`.

Monitoraggio degli endpoint Route 53 Resolver con Amazon CloudWatch

Puoi utilizzare Amazon CloudWatch per monitorare il numero di query DNS inoltrate dagli endpoint Route 53 Resolver. Amazon CloudWatch raccoglie ed elabora dati grezzi in metriche leggibili e quasi in tempo reale. Queste statistiche vengono registrate per un periodo di due settimane, per permettere l'accesso a informazioni storiche e per offrire una prospettiva migliore sulle prestazioni delle risorse. Per impostazione predefinita, i dati metrici per gli endpoint Resolver vengono inviati automaticamente a intervalli di cinque minuti. CloudWatch L'intervallo di cinque minuti è anche l'intervallo più piccolo in cui è possibile inviare i dati dei parametri.

Per ulteriori informazioni su Resolver, consulta Che cos'è Amazon Route 53 Resolver?. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

Parametri e dimensioni per Route 53 Resolver

Quando configuri Resolver per inoltrare le query DNS alla tua rete o viceversa, Resolver inizia a inviare metriche e dimensioni una volta ogni cinque minuti a CloudWatch circa il numero di query che vengono inoltrate. È possibile utilizzare le seguenti procedure per visualizzare le metriche nella console o visualizzarle utilizzando (). CloudWatch AWS Command Line Interface AWS CLI

Per visualizzare le metriche del Resolver utilizzando la console CloudWatch

1. Apri la console all' CloudWatch indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nella barra di navigazione, selezionare la regione dove è stato creato l'endpoint.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Nella scheda All metrics (Tutti i parametri), scegliere Route 53 Resolver.
5. Scegliere By Endpoint (In base a endpoint) per visualizzare conteggi di query per un endpoint specificato. Quindi scegliere gli endpoint dei quali si desidera visualizzare il numero di query.

   Scegli Across All Endpoints per visualizzare i conteggi delle query per tutti gli endpoint in entrata o per tutti gli endpoint in uscita creati dall'account corrente. AWS Quindi scegli InboundQueryVolumeo per visualizzare i conteggi OutboundQueryVolumedesiderati.

Per visualizzare le metriche utilizzando il AWS CLI

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Argomenti

- CloudWatch metriche per Route 53 Resolver
- Dimensioni e parametri per Route 53 Resolver

CloudWatch metriche per Route 53 Resolver

Lo spazio dei nomi `AWS/Route53Resolver` include i parametri per gli endpoint di Route 53 Resolver e per gli indirizzi IP.

Argomenti

Parametri per gli endpoint di Resolver

Lo spazio dei nomi `AWS/Route53Resolver` include i parametri descritti di seguito per endpoint Route 53 Resolver.

EndpointHealthyENICount

Il numero di interfacce di rete elastiche con lo stato `OPERATIONAL`. Ciò significa che le interfacce di rete di Amazon VPC per questo endpoint (specificate da `EndpointId`) sono configurate correttamente e in grado di inoltrare il traffico in entrata e in uscita delle query DNS tra la rete e Resolver.

Statistiche valide: Minima, Massima, Media

Unità: numero

EndpointUnhealthyENICount

Il numero di interfacce di rete elastiche con lo stato `AUTO_RECOVERING`.

Ciò significa che il resolver cerca di ripristinare una o più interfacce di rete di Amazon VPC associate all'endpoint (specificate da `EndpointId`). Durante il processo di ripristino, l'endpoint funziona con capacità limitata e non è in grado di elaborare le query DNS finché non viene ripristinato completamente.

Statistiche valide: Minima, Massima, Media

Unità: numero

InboundQueryVolume

Per gli endpoint in entrata, il numero di query DNS inoltrate dalla rete all'utente tramite l'endpoint specificato da. VPCs `EndpointId`

Statistiche valide: somma

Unità: numero

OutboundQueryVolume

Per gli endpoint in uscita, il numero di query DNS inoltrate dalla rete all'utente tramite l'endpoint specificato da. VPCs `EndpointId`

Statistiche valide: somma

Unità: numero

OutboundQueryAggregateVolume

Per gli endpoint in uscita, il numero totale di query DNS inoltrate da Amazon VPCs alla tua rete, incluse le seguenti:

- Il numero di query DNS inoltrate dalla tua rete attraverso l'endpoint specificato VPCs da. `EndpointId`
- Quando l'account corrente condivide le regole Resolver con altri account, le relative query vengono create da altri account VPCs che vengono inoltrate alla rete tramite l'endpoint specificato da. `EndpointId`

Statistiche valide: somma

Unità: numero

Parametri per gli indirizzi IP di Resolver

Lo spazio dei nomi `AWS/Route53Resolver` include le seguenti metriche per ogni indirizzo IP associato a un endpoint Resolver in ingresso o in uscita. Quando specifichi un endpoint, Resolver crea un'interfaccia di rete elastica di Amazon VPC.

InboundQueryVolume

Per ogni indirizzo IP degli endpoint in ingresso, il numero di query DNS inoltrate dalla rete all'indirizzo IP specificato. Ogni indirizzo IP viene identificato dall'ID dell'indirizzo IP. È possibile ottenere questo valore utilizzando la console Route 53. Nella pagina relativa all'endpoint applicabile, nella sezione Indirizzi IP, vedere la colonna ID indirizzo IP. È inoltre possibile ottenere il valore a livello di codice utilizzando. ListResolverEndpointIpAddresses

Statistiche valide: somma

Unità: numero

OutboundQueryAggregateVolume

Per ogni indirizzo IP per i tuoi endpoint in uscita, il numero totale di query DNS inoltrate da Amazon VPCs alla tua rete, incluse le seguenti:

- Il numero di query DNS inoltrate dalla tua rete utilizzando l'indirizzo IP specificato. VPCs
- Quando l'account corrente condivide le regole del Resolver con altri account, le relative query vengono create da altri account VPCs che vengono inoltrate alla rete utilizzando l'indirizzo IP specificato.

Ogni indirizzo IP viene identificato dall'ID dell'indirizzo IP. È possibile ottenere questo valore utilizzando la console Route 53. Nella pagina relativa all'endpoint applicabile, nella sezione Indirizzi IP, vedere la colonna ID indirizzo IP. È inoltre possibile ottenere il valore a livello di codice utilizzando. ListResolverEndpointIpAddresses

Statistiche valide: somma

Unità: numero

Dimensioni e parametri per Route 53 Resolver

I parametri di Route 53 Resolver per gli endpoint in entrata e in uscita utilizzano lo spazio dei nomi `AWS/Route53Resolver` e forniscono i parametri per `EndpointId`. Se si specifica un valore per la `EndpointId` dimensione, CloudWatch restituisce il numero di query DNS per l'endpoint specificato. Se non lo specifichi`EndpointId`, CloudWatch restituisce il numero di query DNS per tutti gli endpoint creati dall'account corrente. AWS

La dimensione `RniId` è supportata per le metriche `OutboundQueryAggregateVolume` e `InboundQueryVolume`.

Monitoraggio dei gruppi di regole del firewall DNS di Route 53 Resolver con Amazon CloudWatch

Puoi utilizzare Amazon CloudWatch per monitorare il numero di query DNS filtrate dai gruppi di regole del firewall DNS di Route 53 Resolver. Amazon CloudWatch raccoglie ed elabora dati grezzi in metriche leggibili e quasi in tempo reale. Queste statistiche vengono registrate per un periodo di due settimane, per permettere l'accesso a informazioni storiche e per offrire una prospettiva migliore sulle prestazioni delle risorse. Per impostazione predefinita, i dati metrici per i gruppi di regole del firewall DNS vengono inviati automaticamente a intervalli di cinque minuti. CloudWatch

Per ulteriori informazioni su DNS Firewall, consulta Utilizzo di DNS Firewall per filtrare il traffico DNS in uscita. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

Parametri e dimensioni per DNS Firewall per Route 53 Resolver

Quando si associa un gruppo di regole Route 53 Resolver DNS Firewall a un VPC per filtrare le query DNS, DNS Firewall inizia a inviare metriche e dimensioni una volta ogni 5 minuti alle query che filtra. CloudWatch Per informazioni su parametri e dimensioni per DNS Firewall, consulta CloudWatch metriche per Route 53 Resolver DNS Firewall.

È possibile utilizzare le seguenti procedure per visualizzare le metriche nella console o visualizzarle utilizzando (). CloudWatch AWS Command Line Interface AWS CLI

Per visualizzare le metriche del firewall DNS utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Nella barra di navigazione, scegli la regione che desideri visualizzare.
3. Nel riquadro di navigazione, seleziona Parametri.
4. Nella scheda All metrics (Tutti i parametri), scegliere Route 53 Resolver.
5. Seleziona una metrica che ti interessa.

Per visualizzare le metriche utilizzando il AWS CLI

- Al prompt dei comandi, utilizza il comando seguente:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Argomenti

- CloudWatch metriche per Route 53 Resolver DNS Firewall

CloudWatch metriche per Route 53 Resolver DNS Firewall

Lo spazio dei nomi `AWS/Route53Resolver` include i parametri per i gruppi di regole di DNS Firewall per Route 53 Resolver.

Argomenti

Parametri per i gruppi di regole di DNS Firewall per Route 53 Resolver

FirewallRuleGroupQueryVolume

Il numero di query DNS Firewall che corrispondono a un gruppo di regole del firewall (specificato da `FirewallRuleGroupId`).

Dimensioni: `FirewallRuleGroupId`

Statistiche valide: somma

Unità: numero

Metriche per VPCs

VpcFirewallQueryVolume

Il numero di query DNS Firewall da un VPC (specificato da `VpcId`).

Dimensioni: `VpcId`

Statistiche valide: somma

Unità: numero

Parametri per il gruppo di regole del firewall e l'associazione VPC

FirewallRuleGroupVpcQueryVolume

Il numero di query DNS Firewall da un VPC (specificato da `VpcId`) che corrispondono a un gruppo di regole del firewall (specificato da `FirewallRuleGroupId`).

Dimensioni: `FirewallRuleGroupId, VpcId`

Statistiche valide: somma

Unità: numero

Parametri per un elenco di domini in un gruppo di regole del firewall

FirewallRuleQueryVolume

Il numero di query DNS Firewall che corrispondono a un elenco di domini del firewall (specificato da `FirewallDomainListId`) all'interno di un gruppo di regole del firewall (specificato da `FirewallRuleGroupId`).

Dimensioni: `FirewallRuleGroupId, FirewallDomainListId`

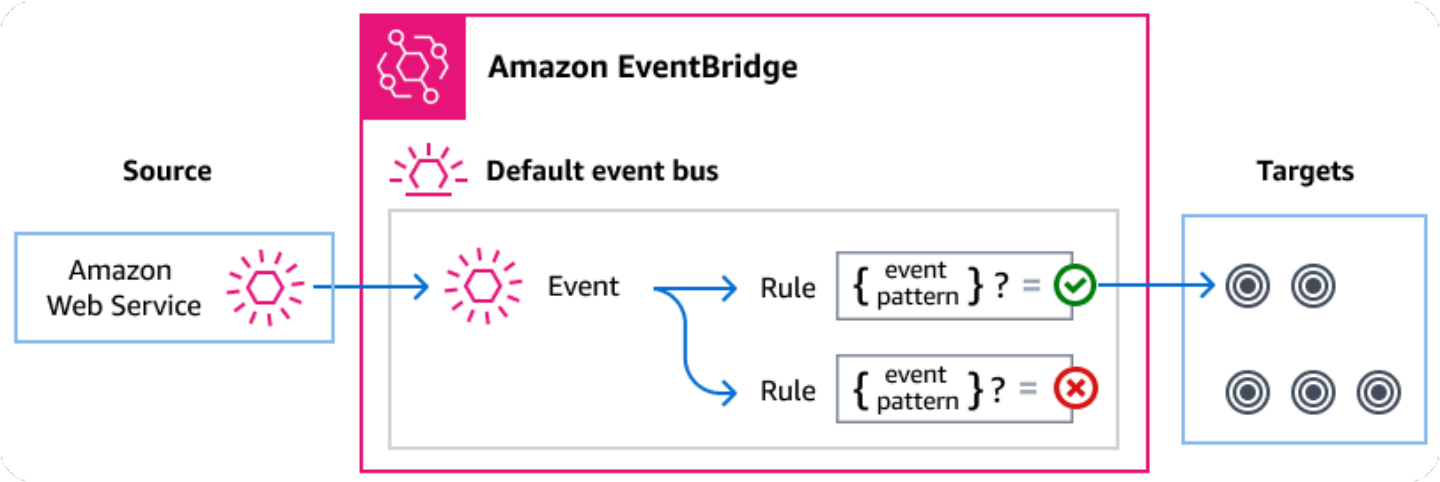
Statistiche valide: somma

Unità: numero

Gestione degli eventi del firewall DNS di Route 53 Resolver utilizzando Amazon EventBridge

Amazon EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti dell'applicazione, semplificando la creazione di applicazioni scalabili basate sugli eventi. L'architettura basata su eventi è uno stile di creazione di sistemi software ad accoppiamento debole che interagiscono emettendo e rispondendo a eventi. Gli eventi rappresentano un cambiamento in una risorsa o in un ambiente.

Come molti AWS servizi, DNS Firewall genera e invia eventi al bus eventi EventBridge predefinito. (Il bus eventi predefinito viene fornito automaticamente in ogni AWS account.) Un router di eventi è un router che riceve eventi e li invia a nessuna o a più destinazioni o target. Le regole specificate per il bus degli eventi valutano gli eventi non appena arrivano. Ogni regola verifica se un evento corrisponde al modello di evento della regola. Se l'evento corrisponde, il bus degli eventi invia l'evento alle destinazioni specificate.



Argomenti

- Eventi del firewall DNS di Route 53 Resolver
- Invio degli eventi del firewall DNS di Route 53 Resolver tramite regole EventBridge
- Amazon EventBridge autorizzazioni
- EventBridge Risorse aggiuntive
- Riferimento dettagliato agli eventi del firewall DNS di Route 53 Resolver

Eventi del firewall DNS di Route 53 Resolver

Route 53 Resolver invia automaticamente gli eventi del firewall DNS al bus eventi predefinito. EventBridge È possibile creare regole sul bus degli eventi; ogni regola include uno schema di eventi e uno o più obiettivi. Gli eventi che corrispondono allo schema di eventi di una regola vengono consegnati agli obiettivi specificati con la massima diligenza possibile. Gli eventi potrebbero essere consegnati fuori servizio.

I seguenti eventi vengono generati da DNS Firewall. Per ulteriori informazioni, consulta EventBridgela Guida per l'Amazon EventBridge utente. .

Tipo di dettaglio dell'evento	Descrizione
Blocco firewall DNS	Qualsiasi azione di blocco eseguita su un dominio.
Avviso firewall DNS	Qualsiasi azione di avviso eseguita su un dominio.

Invio degli eventi del firewall DNS di Route 53 Resolver tramite regole EventBridge

Per fare in modo che il bus degli eventi EventBridge predefinito invii gli eventi del firewall DNS a una destinazione, è necessario creare una regola che contenga un modello di eventi che corrisponda ai dati negli eventi del firewall DNS desiderati.

La creazione di una regola prevede i seguenti passaggi generali:

1. Creazione di un modello di evento per la regola che specifica:
   - Route 53 Resolver è l'origine degli eventi valutati dalla regola.
   - (Facoltativo): qualsiasi altro dato sull'evento con cui confrontarsi.

   Per ulteriori informazioni, consulta ???
2. (Facoltativo): creazione di un trasformatore di input che personalizzi i dati dell'evento prima di EventBridge passare le informazioni alla destinazione della regola.

   Per ulteriori informazioni, consulta Input transformation nella Guida per l'EventBridge utente.
3. Specificare le destinazioni a cui si desidera EventBridge fornire eventi che corrispondono allo schema degli eventi.

   Le destinazioni possono essere altri AWS servizi, applicazioni software-as-a-service (SaaS), destinazioni API o altri endpoint personalizzati. Per ulteriori informazioni, consulta la sezione Destinazioni nella Guida per l'utente di EventBridge .

Per istruzioni complete sulla creazione di regole del bus degli eventi, consulta Creazione di regole che reagiscono agli eventi nella Guida per l'EventBridge utente.

Creazione di modelli di eventi per gli eventi del firewall DNS di Route 53 Resolver

Quando DNS Firewall invia un evento al bus eventi predefinito, EventBridge utilizza il modello di eventi definito per ogni regola per determinare se l'evento deve essere inviato alle destinazioni della regola. Un modello di eventi corrisponde ai dati negli eventi DNS Firewall desiderati. Ogni modello di evento è un oggetto JSON che contiene:

- Un attributo `source` che identifica il servizio che invia l'evento. Per gli eventi DNS Firewall, l'origine è. `aws.route53resolver`
- (Facoltativo): Un attributo `detail-type` che contiene una serie di tipi di eventi da abbinare.

- (Facoltativo): Un attributo `detail` contenente qualsiasi altro dato relativo all'evento da abbinare.

Ad esempio, il seguente schema di eventi corrisponde sia agli eventi di avviso che a quelli di blocco di DNS Firewall:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Mentre il seguente schema di eventi corrisponde a un'azione BLOCK:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS Firewall invia lo stesso evento per lo stesso dominio solo una volta nell'arco di 6 ore. Per esempio:

1. L'istanza i-123 ha inviato una query DNS exampledomain.com all'ora T1. DNS Firewall invia un avviso o un evento di blocco poiché si tratta della prima occorrenza.
2. L'istanza i-123 ha inviato un DNSquery exampledomain.com all'ora T1+30 minuti. DNS Firewall non invia un avviso o blocca un evento poiché si tratta di un evento che si ripete entro la finestra di 6 ore.
3. L'istanza i-123 ha inviato una query DNS exampledomain.com all'orario T1+7 ore. DNS Firewall invia un avviso o un evento di blocco quando questo si verifica al di fuori della finestra di 6 ore.

Per ulteriori informazioni sulla scrittura di modelli di eventi, consulta Event pattern nella Guida per l'EventBridge utente.

Test dei modelli di eventi per gli eventi del firewall DNS in EventBridge

È possibile utilizzare la EventBridge Sandbox per definire e testare rapidamente un pattern di eventi, senza dover completare il processo più ampio di creazione o modifica di una regola. Utilizzando la Sandbox, è possibile definire un pattern di eventi e utilizzare un evento di esempio per confermare che il pattern corrisponda agli eventi desiderati. EventBridge ti danno la possibilità di creare una nuova regola usando quel pattern di eventi, direttamente dalla sandbox.

Per ulteriori informazioni, consulta Testare un pattern di eventi utilizzando la EventBridge sandbox nella Guida per l'EventBridge utente.

Creazione di una EventBridge regola e di un obiettivo per DNS Firewall

La procedura seguente mostra come creare una regola che EventBridge consenta di inviare eventi per tutte le azioni di avviso e blocco del firewall DNS e aggiungere una AWS Lambda funzione come destinazione per la regola.

1. Usa AWS CLI per creare una EventBridge regola:

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. Associa una funzione Lambda come obiettivo per la regola:

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Per aggiungere le autorizzazioni necessarie per richiamare la destinazione, esegui il seguente comando Lambda: AWS CLI

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge autorizzazioni

DNS Firewall non richiede autorizzazioni aggiuntive per fornire eventi. Amazon EventBridge

Le destinazioni specificate potrebbero richiedere autorizzazioni o configurazioni specifiche. Per maggiori dettagli sull'utilizzo di servizi specifici per gli obiettivi, consulta Amazon EventBridge gli obiettivi nella Guida per l'Amazon EventBridge utente.

EventBridge Risorse aggiuntive

Fate riferimento ai seguenti argomenti della Guida per Amazon EventBridge l'utente per ulteriori informazioni su come utilizzare EventBridge per elaborare e gestire gli eventi.

- Per informazioni dettagliate sul funzionamento degli event bus, consulta Amazon EventBridge Event Bus.
- Per informazioni sulla struttura degli eventi, consulta Eventi.
- Per informazioni sulla creazione di modelli di eventi EventBridge da utilizzare per abbinare gli eventi alle regole, consulta Modelli di eventi.
- Per informazioni sulla creazione di regole per specificare quali eventi vengono EventBridge elaborati, consulta Regole.
- Per informazioni su come specificare a quali servizi o altre destinazioni vengono EventBridge inviati gli eventi corrispondenti, consulta Target.

Riferimento dettagliato agli eventi del firewall DNS di Route 53 Resolver

Tutti gli eventi generati dai AWS servizi dispongono di un set comune di campi contenenti metadati relativi all'evento, ad esempio il AWS servizio da cui è generato l'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è verificato l'evento e altri. Per le definizioni di questi campi generali, consultate il riferimento alla struttura degli eventi nella Guida per l'Amazon EventBridge utente.

Inoltre, ogni evento ha un campo `detail` che contiene dati specifici per quel particolare evento. Il riferimento seguente definisce i campi di dettaglio per i vari eventi del firewall DNS.

Quando si utilizza EventBridge per selezionare e gestire gli eventi del firewall DNS, è utile tenere presente quanto segue:

- Il `source` campo per tutti gli eventi di DNS Firewall è impostato su. `aws.route53resolver`
- Il campo `detail-type` specifica il tipo di evento.

  Ad esempio `DNS Firewall Block` o `DNS Firewall Alert`.
- Il campo `detail` contiene i dati specifici di quel particolare evento.

Per informazioni sulla creazione di modelli di eventi che consentono alle regole di corrispondere agli eventi del firewall DNS, consulta la sezione Modelli di eventi nella Guida per l'Amazon EventBridge utente.

Per ulteriori informazioni sugli eventi e su come li EventBridge elabora, consulta Amazon EventBridge gli eventi nella Guida per l'Amazon EventBridge utente.

Argomenti

Dettagli dell'evento di avviso DNS Firewall

Di seguito sono riportati i campi di dettaglio per i dettagli dell'evento Alert status.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per gli eventi Route 53.

```
{...,
 "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

Identifica il tipo di evento.

Per questo evento, questo valore è`DNS Firewall Alert`.

`source`

Identifica il servizio che ha generato l'evento. Per gli eventi DNS Firewall, questo valore è`aws.route53resolver`.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per questo evento, questi dati includono:

`account-id`

L'ID di chi Account AWS ha creato il VPC.

`last-observed-at`

Il timestamp di quando è stata effettuata la query Alert/Block nel VPC.

`query-name`

Il nome di dominio (esempio.com) o di sottodominio (www.esempio.com) specificato nella query.

`query-type`

Il tipo di record DNS specificato nella richiesta o QUALSIASI. Per ulteriori informazioni sui tipi supportati da Route 53, consulta Tipi di record DNS supportati.

`query-class`

La classe della query.

`transport`

Il protocollo utilizzato per inviare la query DNS.

`firewall-rule-action`

L'operazione specificata dalla regola che corrisponde al nome di dominio nella query. `ALERT` o `BLOCK`.

`firewall-rule-group-id`

L'ID del gruppo di regole di DNS Firewall che corrisponde al nome di dominio nella query. Per ulteriori informazioni sui gruppi di regole del firewall, vedere DNS Firewall. Gruppi di regole e regole in DNS Firewall

`firewall-domain-list-id`

L'elenco di domini utilizzato dalla regola che corrisponde al nome di dominio nella query.

`firewall-protection`

Protezione DNS Firewall Advanced, DGA o DNS_TUNNELING. Per ulteriori informazioni, consulta DNS Firewall. Route 53 Resolver DNS Firewall avanzato

`resourcese`

Contiene i tipi di risorse e dettagli aggiuntivi su di essi.

`resource-type`

Specifica il tipo di risorsa, ad esempio un endpoint resolver o un'istanza VPC.

`resource-type``-detail`

Dettagli aggiuntivi sulla risorsa.

Example Evento di avviso DNS Firewall

Di seguito è riportato un esempio di evento di avviso.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
```

```
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DGA",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```

Dettagli dell'evento di blocco del firewall DNS

Di seguito sono riportati i campi di dettaglio per*`event name`*.

I `detail-type` campi `source` e sono inclusi perché contengono valori specifici per gli eventi della Route 53.

```
{...,
 "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
```

```
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

Identifica il tipo di evento.

Per questo evento, questo valore è`DNS Firewall Alert`.

`source`

Identifica il servizio che ha generato l'evento. Per gli eventi DNS Firewall, questo valore è`aws.route53resolver`.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per questo evento, questi dati includono:

`account-id`

L'ID di chi Account AWS ha creato il VPC.

`last-observed-at`

Il timestamp di quando è stata effettuata la query Alert/Block nel VPC.

`query-name`

Il nome di dominio (esempio.com) o di sottodominio (www.esempio.com) specificato nella query.

`query-type`

Il tipo di record DNS specificato nella richiesta o QUALSIASI. Per ulteriori informazioni sui tipi supportati da Route 53, consulta Tipi di record DNS supportati.

`query-class`

La classe della query.

`transport`

Il protocollo utilizzato per inviare la query DNS.

`firewall-rule-action`

L'operazione specificata dalla regola che corrisponde al nome di dominio nella query. `ALERT` o `BLOCK`.

`firewall-rule-group-id`

L'ID del gruppo di regole di DNS Firewall che corrisponde al nome di dominio nella query. Per ulteriori informazioni sui gruppi di regole del firewall, vedere DNS Firewall. Gruppi di regole e regole in DNS Firewall

`firewall-domain-list-id`

L'elenco di domini utilizzato dalla regola che corrisponde al nome di dominio nella query.

`firewall-protection`

Protezione DNS Firewall Advanced, DGA o DNS_TUNNELING. Per ulteriori informazioni, consulta DNS Firewall. Route 53 Resolver DNS Firewall avanzato

`resourcese`

Contiene i tipi di risorse e dettagli aggiuntivi su di essi.

`resource-type`

Specifica il tipo di risorsa, ad esempio un endpoint resolver o un'istanza VPC.

resource-type-detail

Dettagli aggiuntivi sulla risorsa.

Example Esempio di evento

Di seguito è riportato un esempio di evento a blocchi.


```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DNS_TUNNELING",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
```

```
"vpc-id": "vpc-7example"
 }
}
```

Registrazione delle chiamate API Amazon Route 53 con AWS CloudTrail

Route 53 è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Route 53. CloudTrail acquisisce tutte le chiamate API per Route 53 come eventi, incluse le chiamate dalla console Route 53 e le chiamate in codice verso Route 53 APIs. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Route 53. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata a Route 53, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Argomenti

Informazioni sulla Route 53 in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Route 53, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Route 53, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail sarà valido in tutte le regioni. Il trail registra gli eventi da tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso

- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Route 53 vengono registrate CloudTrail e documentate nell'Amazon Route 53 API Reference. Ad esempio, le chiamate alle `RegisterDomain` azioni `CreateHostedZone` `CreateHealthCheck`, e generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Visualizzazione di eventi di Route 53 nella cronologia eventi

CloudTrail consente di visualizzare gli eventi recenti nella cronologia degli eventi. Per visualizzare gli eventi per le richieste API di Route 53, è necessario scegliere Stati Uniti orientali (Virginia settentrionale) nel selettore delle regioni nella parte superiore della console. Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Informazioni sulle voci dei file di log di Route 53

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'elemento `eventName` identifica l'operazione che si è verificata. (Nei CloudTrail log, la prima lettera è minuscola per le azioni di registrazione del dominio, anche se è maiuscola nei nomi delle azioni. Ad esempio, `UpdateDomainContact` appare come `updateDomainContact` nei log). CloudTrail supporta tutte le azioni dell'API Route 53. L'esempio seguente mostra una voce di CloudTrail registro che illustra le seguenti azioni:

- Elenca le zone ospitate associate a un account AWS
- Crea un controllo dell'integrità
- Crea due record
- Elimina una zona ospitata
- Aggiorna le informazioni per un dominio registrato
- Creazione di un endpoint in uscita di 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"
        }
    ]
}
```

Risoluzione dei problemi di Amazon Route 53

Questa pagina tratta i seguenti argomenti di risoluzione dei problemi per Amazon Route 53:

1. Indisponibilità del dominio:
   - Comprendi i motivi più comuni per cui il tuo dominio potrebbe non essere disponibile su Internet, ad esempio la mancata conferma dell'e-mail del registrante, i problemi di trasferimento del servizio DNS, le impostazioni errate del name server o l'eliminazione delle zone ospitate.
2. Sospensione del dominio:
   - Scopri le cause della sospensione (ClientHold stato) del dominio e come annullare la sospensione del dominio, inclusi domini scaduti, modifiche non verificate all'indirizzo email del registrante e problemi di elaborazione dei pagamenti.
3. Trasferimento del dominio non riuscito:
   - Scopri i motivi più comuni alla base di un trasferimento di dominio fallito su Route 53, ad esempio la mancata autorizzazione del trasferimento, codici di autorizzazione non validi o problemi con i nomi di dominio internazionalizzati.
4. Le impostazioni DNS non hanno effetto:
   - Risolvi le situazioni in cui le modifiche alle impostazioni DNS non hanno ancora avuto effetto, tra cui la memorizzazione nella cache del resolver DNS, gli aggiornamenti errati dei name server e più zone ospitate con lo stesso nome.
5. Errore «Server non trovato»:
   - Trova soluzioni per gli errori «Server Not Found» nel tuo browser, ad esempio record mancanti, valori dei record errati o risorse non disponibili.
6. Instradamento del traffico verso i bucket S3:
   - Risolvi i problemi che si verificano quando tenti di indirizzare il traffico verso un bucket Amazon S3 configurato per l'hosting di siti Web.
7. Problemi di fatturazione:
   - Comprendi gli scenari di fatturazione più comuni, tra cui la fatturazione doppia per la stessa zona ospitata, le fatture multiple per i domini e i problemi relativi alla registrazione del dominio quando il dominio è chiuso o Account AWS è definitivamente chiuso.

Argomenti

Il mio dominio non è disponibile su Internet

Di seguito sono descritti i motivi più comuni per cui il tuo dominio non è disponibile su Internet.

Argomenti

Hai registrato un nuovo dominio, ma non hai fatto clic sul link contenuto nel messaggio e-mail di conferma

Quando si registra un nuovo dominio, ICANN richiede la conferma che l'indirizzo e-mail di contatto per il registrant è valido. Per ottenere la conferma, inviamo un'e-mail contenente un link. (Se non rispondi alla prima e-mail, reinviamo la stessa e-mail fino a due o più volte.) Hai tra 3 e 15 giorni per fare clic sul collegamento, a seconda del dominio di primo livello. Dopodiché, il collegamento smette di funzionare.

Se non fai clic sul link contenuto nel messaggio e-mail nell'intervallo di tempo specificato, ICANN richiede di sospendere il dominio. Per informazioni su come eseguire inviare nuovamente l'e-mail di conferma al contatto del registrant, consulta Rinvio di e-mail di autorizzazione e di conferma.

Hai trasferito la registrazione di dominio ad Amazon Route 53, ma non il servizio DNS

Se il tuo registrar precedente ha offerto gratuitamente il servizio DNS con la registrazione del dominio, potrebbe aver interrotto la fornitura del servizio DNS quando hai trasferito la registrazione del dominio a Route 53. Esegui la procedura seguente per determinare se questo è il problema e, in caso affermativo, per risolvere il problema.

Come ripristinare il servizio DNS se il tuo precedente registrar lo ha annullato dopo il trasferimento della registrazione del dominio a Route 53

1. Contatta il tuo precedente registrar e conferma che ha annullato il servizio DNS per il tuo dominio. In questo caso ci sono tre modi più rapidi per ripristinare il servizio DNS per il dominio, in ordine di auspicabilità:

   - Se il registrar precedente fornisce il servizio DNS a pagamento, chiedigli di ripristinare il servizio DNS utilizzando i vecchi record DNS e server di nomi per il tuo dominio.
   - Se il registrar precedente non fornisce il servizio DNS a pagamento senza la registrazione del dominio, chiedi se è possibile trasferire la registrazione del dominio nuovamente al registrar e ripristinare il servizio DNS utilizzando i vecchi record DNS e server di nomi per il tuo dominio.
   - Se puoi ritrasferire la registrazione di dominio al precedente registrar ma il registrar non ha più i tuoi record DNS, chiedi se è possibile ritrasferire la registrazione di dominio e ottenere lo stesso set server di nomi precedentemente assegnati al dominio. Se questo è possibile, sarà necessario ricreare i vecchi record DNS. Tuttavia, non appena lo fai, il tuo dominio tornerà disponibile.

   Se il tuo precedente registrar non è in grado di aiutarti con qualsiasi di queste opzioni, continua con il passaggio 2.

   > **Important**
   >
   > Se non sei in grado di ripristinare il servizio DNS utilizzando i server di nomi specificati quando hai trasferito il tuo dominio a Route 53, affinché il tuo dominio diventi

nuovamente disponibile su Internet possono essere necessari fino a due giorni dopo l'esecuzione dei passaggi rimanenti della procedura. Di solito, i resolver DNS memorizzano nella cache i server di nomi per un nome di dominio per 24-48 ore, e occorre questo tempo affinché i resolver DNS ottengano i nomi dei nuovi server di nomi.

2. Scegli un nuovo servizio DNS, ad esempio, Route 53.
3. Utilizzando il metodo fornito dal nuovo servizio DNS, crea una zona ospitata e record:

   a. Crea una zona ospitata con lo stesso nome di dominio, ad esempio esempio.com.

   b. Utilizza il file di zona che hai ottenuto dal precedente registrar per creare record.

   Se hai scelto Route 53 come tuo nuovo servizio DNS, puoi creare i record importando i file di zona. Per ulteriori informazioni, consulta Creazione di record mediante importazione di un file di zona.
4. Ottieni i server di nomi per la nuova hosted zone. Se hai scelto Route 53 come servizio DNS, consulta Ottenere i server di nomi per una zona ospitata pubblica.
5. Cambia i nomi di server per il tuo dominio con i server di nomi che hai ricevuto nel passaggio 4. Per ulteriori informazioni, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.

Hai trasferito la registrazione del dominio e hai indicato i server di nomi errati nelle impostazioni di dominio

Quando esegui il trasferimento della registrazione di dominio ad Amazon Route 53, una delle impostazioni che è necessario specificare per il dominio è il nome del set di server dei nomi in grado di rispondere alle query DNS per il dominio. Questi server di nomi provengono dalla zona ospitata che la lo stesso nome del dominio. La zona ospitata contiene informazioni su come si desidera instradare il traffico per il dominio, ad esempio l'indirizzo IP di un server Web per www.esempio.com.

È possibile che sia stato specificato accidentalmente i server di nomi per la zona ospitata sbagliata, cosa particolarmente probabile se si dispone di più di una zona ospitata con lo stesso nome del dominio. Per confermare che il dominio sta utilizzando i server di nomi per la corretta zona ospitata e, se necessario, aggiornare i server di nomi per il dominio, eseguire le seguenti procedure.

> **Important**
>
> Se quando hai trasferito il dominio a Route 53 hai specificato i record dei server dei nomi sbagliati, prima che il servizio DNS sia completamente ripristinato, possono essere necessari due giorni dopo la correzione dei server di nomi per il dominio. Questo perché i resolver DNS su Internet in genere richiedono i server di nomi solo una volta ogni due giorni e memorizzano nella cache le risposte.

Come ottenere i server di nomi per la tua hosted zone

1. Se usi un altro servizio DNS per il dominio, utilizza il metodo fornito dal servizio DNS per ottenere i server di nomi per la zona ospitata. Quindi passa alla procedura successiva.

   Se utilizzi Route 53 come servizio DNS per il dominio, accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate).
3. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata.

   > **Important**
   >
   > Se disponi di più di una zona ospitata con lo stesso nome, assicurati di ottenere i server di nomi per la corretta hosted zone.
4. Nel riquadro destro, annota i quattro server indicati per Name Servers (Server di nomi).

Per confermare che il dominio stia utilizzando i server di nomi corretti

1. Se utilizzi un altro servizio DNS per il dominio, accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/

   Se usi Route 53, passa alla fase successiva.
2. Nel riquadro di navigazione, selezionare Registered Domains (Domini registrati).
3. Seleziona il nome del dominio per cui desideri modificare le impostazioni.
4. Scegli Add or Edit Name Servers (Aggiungi o modifica server di nomi).

5. Confronta l'elenco dei server di nomi che hai ottenuto nella procedura precedente con quelli elencati nella finestra di dialogo Edit Name Servers for (Modifica server di nomi per) per il nome di dominio.
6. Se i server di nomi elencati in questa pagina non corrispondono a quelli che hai ricevuto nella procedura precedente, modificali qui e seleziona Update (Aggiorna).

Hai prima trasferito il servizio DNS, ma non hai aspettato abbastanza a lungo prima di trasferire la registrazione del dominio

Una volta trasferito il servizio DNS ad Amazon Route 53 o a un altro servizio DNS, per utilizzare i server di nomi per il nuovo servizio DNS dovrai aggiornare la configurazione per il tuo dominio con il registrar del dominio.

I resolver DNS che rispondono alle richieste per il tuo dominio comunemente memorizzano nella cache i nomi dei server di nomi per 24-48 ore. Se modifichi il servizio DNS per un dominio e sostituisci i server di nomi da un servizio DNS con i server di nomi per un altro servizio DNS, possono essere necessarie fino a 48 ore prima che i resolver DNS inizino a usare i nuovi server di nomi e, di conseguenza, il nuovo servizio DNS.

Ecco come il trasferimento del servizio DNS e quindi il trasferire del tuo dominio troppo presto può causare la non disponibilità del dominio su Internet:

1. Hai trasferito il servizio DNS per il tuo dominio.
2. Hai trasferito il tuo dominio a Route 53 prima che i resolver DNS abbiano iniziato a utilizzare i server di nomi per il tuo nuovo servizio DNS.
3. Il tuo precedente registrar ha annullato il servizio DNS per il tuo dominio non appena il dominio è stato trasferito a Route 53.
4. I resolver DNS stanno ancora instradando query al tuo vecchio servizio DNS, ma non ci sono più record che indicano come instradare il traffico.

Quando la memorizzazione nella cache scade per i server di nomi per il servizio DNS precedente, il DNS inizierà a utilizzare il tuo nuovo servizio DNS. Purtroppo, non vi è alcun modo per accelerare la procedura.

Hai eliminato la zona ospitata utilizzata da Route 53 per instradare il traffico Internet per il dominio

Se Route 53 è il servizio DNS per il dominio ed elimini la zona ospitata utilizzata per instradare il traffico Internet per il dominio, il dominio non sarà disponibile su Internet. Ciò è valido anche se il dominio è registrato con Route 53.

> **Important**
>
> Il ripristino di servizi Internet per il dominio può richiedere fino a 48 ore.

Come ripristinare il servizio Internet se si elimina una zona ospitata utilizzata da Route 53 per instradare il traffico Internet per un dominio

1. Crea un'altra zona ospitata con lo stesso nome del dominio. Per ulteriori informazioni, consulta Creazione di una zona ospitata pubblica.
2. Ricrea i record che si trovavano nella zona ospitata eliminata. Per ulteriori informazioni, consulta Utilizzo dei record.
3. Ottieni i nomi dei server dei nomi che Route 53 ha assegnato alla nuova zona ospitata. Per ulteriori informazioni, consulta Ottenere i server di nomi per una zona ospitata pubblica.
4. Aggiorna la registrazione del dominio per utilizzare i server di nomi ottenuti nella fase 3.
   - Se il dominio è registrato con Route 53, consulta Aggiunta o modifica di server di nomi e glue record per un dominio.
   - Se il dominio è registrato con un altro registrar del dominio, utilizza il metodo fornito dal registrar per aggiornare la registrazione del dominio per utilizzare i nuovi server dei nomi.
5. Attendi il TTL per i server dei nomi da passare ai resolver ricorsivi che hanno memorizzato nella cache i nomi dei server dei nomi per la zona ospitata eliminata. Una volta passato il TTL, quando un browser o un'applicazione inoltra una query DNS per il dominio o uno dei suoi sottodomini, un resolver ricorsivo inoltra la query ai server dei nomi di Route 53 per la nuova zona ospitata. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

   Il TTL per i server dei nomi può avere una durata di 48 ore, a seconda del TLD del dominio.

Il tuo dominio è stato sospeso

Il tuo dominio potrebbe essere non disponibile su Internet perché abbiamo dovuto sospenderlo. Per ulteriori informazioni, consulta Il mio dominio è sospeso (lo stato è ClientHold).

Il mio dominio è sospeso (lo stato è ClientHold)

Se Amazon Route 53 sospende il tuo dominio, il dominio diventa non disponibile su Internet. Puoi usare uno dei seguenti metodi per determinare se un dominio è stato sospeso:

- Nella pagina Domini registrati della console Route 53, individua il nome di dominio nella tabella Avvisi nella parte inferiore della pagina. Se il valore della colonna Status (Stato) è clientHold, il dominio è stato sospeso.
- Invia una query WHOIS per il dominio. Se il valore della colonna Domain Status (Stato del dominio) è clientHold, il dominio è stato sospeso. Il comando WHOIS è disponibile in molti sistemi operativi, ed è disponibile anche come applicazione Web su molti siti web.

Inoltre, quando sospendi un dominio, generalmente inviamo un'e-mail all'indirizzo e-mail di contatto del registrant per il dominio. Tuttavia, se il dominio è stato sospeso in base a un ordine di tribunale, il tribunale potrebbe non consentirci di notificare il registrant.

Per rendere un dominio disponibile su Internet, è necessario annullare la sospensione. Di seguito sono descritti i motivi per cui un dominio può essere sospeso e come annullare la sospensione.

> **Note**
>
> Se hai bisogno di aiuto per annullare la sospensione del tuo dominio, puoi contattare l' AWS assistenza gratuitamente. Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Argomenti

- Hai registrato un nuovo dominio, ma non hai fatto clic sul link contenuto nel messaggio e-mail di conferma
- Hai disattivato il rinnovo automatico per il dominio e il dominio è scaduto
- Hai modificato il tuo indirizzo e-mail di contatto per il registrante, ma non hai verificato che il nuovo indirizzo e-mail sia valido

- Non è stato possibile elaborare il pagamento per il rinnovo automatico del dominio e il dominio è scaduto
- Abbiamo sospeso il dominio per una violazione delle regole di utilizzo di AWS
- Abbiamo sospeso il dominio a causa di un ordine di tribunale

Hai registrato un nuovo dominio, ma non hai fatto clic sul link contenuto nel messaggio e-mail di conferma

Quando registri un dominio con AWS per la prima volta, ICANN richiede che riceviamo la conferma della validità dell'indirizzo e-mail per il contatto del registrante. Per ottenere la conferma, inviamo un'e-mail contenente un link. Hai tra 3 e 15 giorni per fare clic sul collegamento, a seconda del dominio di primo livello. Dopodiché, il collegamento smette di funzionare.

> **Note**
>
> Se hai già registrato uno o più domini con Amazon Route 53 e utilizzi lo stesso indirizzo e-mail per il registrant, non invieremo alcun messaggio e-mail di conferma.

Se non fai clic sul link contenuto nel messaggio e-mail nell'intervallo di tempo specificato, ICANN richiede di sospendere il dominio. Per informazioni su come eseguire inviare nuovamente l'e-mail di conferma al contatto del registrant, consulta Rinvio di e-mail di autorizzazione e di conferma. Quando confermi che l'indirizzo e-mail è valido, annulliamo automaticamente la sospensione del dominio.

Hai disattivato il rinnovo automatico per il dominio e il dominio è scaduto

Quando il rinnovo automatico è abilitato per un dominio (il valore di default per un dominio nuovo o trasferito), rinnoviamo automaticamente la registrazione per il dominio poco prima della data di scadenza. Se disabiliti il rinnovo automatico, inviamo all'indirizzo e-mail di contatto per il registrant tre e-mail promemoria indicando che la registrazione di dominio scadrà. Iniziamo a inviare queste e-mail 45 giorni prima della scadenza del dominio.

Se disabiliti il rinnovo automatico per il dominio e non estendi manualmente il periodo di registrazione per il dominio, generalmente sospendiamo il dominio alla data di scadenza. Si noti che i record per alcuni domini eliminano il dominio anche prima della data di scadenza.

Per informazioni su come rinnovare un dominio scaduto, consulta Rinnovo della registrazione di un dominio.

Hai modificato il tuo indirizzo e-mail di contatto per il registrante, ma non hai verificato che il nuovo indirizzo e-mail sia valido

Se decidi di modificare l'indirizzo e-mail di contatto per il registrante con un indirizzo che non hai già verificato, ICANN richiede conferma che l'indirizzo e-mail di contatto per il registrante sia valido. Per ottenere la conferma, inviamo un'e-mail contenente un link. Hai tra 3 e 15 giorni per fare clic sul collegamento, a seconda del dominio di primo livello. Dopodiché, il collegamento smette di funzionare.

Se non fai clic sul link contenuto nel messaggio e-mail nel periodo di tempo stabilito dal record TLD, ICANN richiede la sospensione del dominio. Per informazioni su come eseguire inviare nuovamente l'e-mail di conferma al contatto del registrant, consulta Rinvio di e-mail di autorizzazione e di conferma. Quando confermi che l'indirizzo e-mail è valido, annulliamo automaticamente la sospensione del dominio.

Non è stato possibile elaborare il pagamento per il rinnovo automatico del dominio e il dominio è scaduto

Se il rinnovo automatico è abilitato per un dominio, ma non siamo stati in grado di elaborare il pagamento (ad esempio, perché i dati della tua carta di credito sono scaduti), inviamo diverse e-mail all'indirizzo e-mail di contatto del registrant per il dominio. Se non riceviamo il pagamento, generalmente sospendiamo il dominio alla data di scadenza. Si noti che i record per alcuni domini eliminano il dominio anche prima della data di scadenza.

Per informazioni su come rinnovare un dominio scaduto, consulta Rinnovo della registrazione di un dominio.

Abbiamo sospeso il dominio per una violazione delle regole di utilizzo di AWS

In caso di sospensione di un dominio per una violazione della Policy di utilizzo di AWS, invieremo una notifica tramite e-mail al contatto registrant per il dominio. (Non inviamo un'e-mail di notifica se l' AWS account è già sospeso per frode.)

Per contestare una sospensione, invia un'email a trustandsafety@support.aws.com.

Abbiamo sospeso il dominio a causa di un ordine di tribunale

Se un dominio è sospeso a causa di un ordine di tribunale, non siamo in grado di annullare la sospensione del dominio fino a quando l'ordine di tribunale non è stato revocato. Per contestare la validità di un'ordinanza del tribunale, invia un'e-mail a trustandsafety@support.aws.com e allega i documenti applicabili.

Trasferimento del dominio di Amazon Route 53 non riuscito

Di seguito sono elencati alcuni dei motivi più comuni per cui il trasferimento di un dominio ad Amazon Route 53 ha esito negativo.

Argomenti

Non hai fatto clic sul link nell'e-mail di autorizzazione

Quando si esegue il trasferimento della registrazione di dominio ad Amazon Route 53, ICANN, l'ente che disciplina la registrazione dei domini, ci richiede di ottenere l'autorizzazione per il trasferimento dal registrant del dominio. Per ottenere l'autorizzazione inviamo un'e-mail contenente un link. Hai tra 5 e 15 giorni per fare clic sul collegamento, a seconda del dominio di primo livello. Dopodiché, il collegamento smette di funzionare.

Se non fai clic sul link contenuto nel messaggio e-mail nell'intervallo di tempo specificato, ICANN richiede di annullare il trasferimento. Per informazioni su come eseguire inviare nuovamente l'e-mail di autorizzazione al contatto del registrant, consulta Rinvio di e-mail di autorizzazione e di conferma.

Il codice di autorizzazione che hai ricevuto dal tuo attuale registrar non è valido

Se richiedi il trasferimento di un dominio ad Amazon Route 53 e non ricevi l'e-mail di autorizzazione, controlla la pagina di stato nella console Route 53. Se la pagina di stato mostra che il codice di autorizzazione di trasferimento fornito dal registrar non è valido, esegui i seguenti passaggi:

1. Contatta l'attuale registrar per il dominio per richiedere un nuovo codice di autorizzazione. Conferma quanto segue:
   - Per quanto tempo il nuovo codice di autorizzazione rimarrà attivo. È necessario richiedere un trasferimento di dominio prima della scadenza del codice.
   - Il nuovo codice di autorizzazione è diverso dal codice che non è valido. In caso contrario, richiedi all'attuale registrar di aggiornare il codice di autorizzazione.
2. Invia un'altra richiesta per trasferire il dominio. Per ulteriori informazioni, consulta Fase 5: Richiedi il trasferimento nell'argomento Trasferimento della registrazione per un dominio ad Amazon Route 53.

Errore "Parameters in request are not valid" (Parametri nella richiesta non validi) durante il trasferimento di un dominio .es ad Amazon Route 53

Amazon Route 53 restituisce un errore "Parameters in request are not valid" (Parametri nella richiesta non validi) durante il tentativo di trasferimento di un dominio .es a Route 53 e il tipo di contatto del registrant è Società. Per completare il trasferimento, modifica il tipo di contatto del registrante in Persona, quindi invia nuovamente.

Il nome di dominio internazionalizzato che stai trasferendo su Amazon Route 53 è elencato in punycode?

Quando si registra un nuovo nome dominio o si creano zone ospitate e registri, è possibile specificare lettere diverse da a-z (ad esempio, la ç francese), caratteri in altri alfabeti (per esempio, cirillico o arabo) e caratteri in cinese, giapponese o coreano. Amazon Route 53 memorizza questi nomi di dominio internazionalizzati (IDNs) in Punycode, che rappresenta i caratteri Unicode come stringhe ASCII.

Se ricevi un errore durante il trasferimento di un file su Route 53, usa IDNs punycode per rappresentarlo e riprova. Per ulteriori informazioni, consulta Formattazione di nomi dominio internazionalizzati.

Ho cambiato le impostazioni DNS, ma non sono state applicate

Se hai modificato le impostazioni DNS, di seguito sono elencati alcuni dei motivi più comuni per cui le modifiche non sono state ancora applicate.

Argomenti

Hai trasferito il servizio DNS ad Amazon Route 53 nelle ultime 48 ore, quindi il DNS sta ancora utilizzando il servizio DNS precedente

Una volta trasferito il servizio DNS ad Amazon Route 53, hai utilizzato il metodo fornito dal registrar per il tuo dominio per sostituire i server di nomi per il servizio DNS precedente con i quattro server di nomi per Route 53.

> **Note**
>
> Se non sei sicuro di averlo fatto, consulta Hai recentemente trasferito il servizio DNS ad Amazon Route 53, ma non hai aggiornato i server di nomi con il registrar del dominio.

Di solito, i registrar usano un TTL di 24-48 ore per i server di nomi. Ciò significa che quando un resolver DNS ottiene i server di nomi per il tuo dominio, utilizza queste informazioni per un massimo di 48 ore prima di inviare un'altra richiesta per gli attuali server di nomi per il dominio. Se hai trasferito il servizio DNS a Route 53 nelle ultime 48 ore e quindi hai modificato le impostazioni DNS, alcuni

resolver DNS continueranno a utilizzare il tuo vecchio servizio DNS per instradare il traffico per il dominio.

Hai recentemente trasferito il servizio DNS ad Amazon Route 53, ma non hai aggiornato i server di nomi con il registrar del dominio

Il registrar per il tuo dominio dispone di una serie di informazioni sul dominio, tra cui i server di nomi per il servizio DNS per il dominio. Di solito, il registrar del dominio è anche il tuo servizio DNS, pertanto i server di nomi che sono associati con il tuo dominio appartengono al registrar. Questi server di nomi indicano a DNS dove ottenere informazioni sul modo in cui desideri che il traffico per il tuo dominio venga instradato, ad esempio, all'indirizzo IP di un server Web per il tuo dominio.

Quando trasferisci il servizio DNS ad Amazon Route 53, devi utilizzare il metodo che viene fornito dal registrar del tuo dominio per modificare i server di nomi che sono associati al tuo dominio. In genere sostituisci i server di nomi che vengono forniti dal registrar con i quattro server di nomi di Route 53 che sono associati alle zone ospitate create per il dominio.

Se hai creato una nuova zona ospitata e record per il tuo dominio e hai specificato impostazioni differenti rispetto a quelle utilizzate per il servizio DNS precedente e se il DNS sta ancora instradando il traffico alle vecchie risorse, è possibile che tu non abbia aggiornato i server di nomi con il registrar del dominio. Per stabilire se il registrar sta utilizzando i server dei nomi per la zona ospitata di Route 53 corretta e, se necessario, aggiornare i server dei nomi per il dominio, completa le seguenti procedure.

Per ottenere i server di nomi per la tua zona ospitata e aggiornare l'impostazione del server di nomi con il registrar del dominio

1. Accedi AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nel riquadro di navigazione scegliere Hosted Zones (Zone ospitate).
3. Nella pagina Zone ospitate, scegli il nome (non il pulsante di opzione) per la zona ospitata.

   > **Important**
   >
   > Se disponi di più di una zona ospitata con lo stesso nome, assicurati di ottenere i server di nomi per la corretta hosted zone.

4. Nell'elenco Nome record, prendi nota dei quattro server riportati per Server dei nomi.

5. Utilizzando il metodo fornito dal registrar per il dominio, visualizza l'elenco dei server di nomi per il dominio.
6. Se i server di nomi per il dominio corrispondono ai server di nomi che hai ricevuto al passo 4, la configurazione del dominio è corretta.

   Se i server dei nomi per il dominio non corrispondono ai server dei nomi che hai ottenuto alla fase 4, aggiorna il dominio in modo da utilizzare i server dei nomi di Route 53.
7.

> **Important**
>
> Quando modifichi i server dei nomi per il dominio con i server dei nomi della tua zona ospitata di Route 53, possono essere necessari fino a due giorni affinché la modifica diventi effettiva e affinché Route 53 diventi il servizio DNS. Questo perché i resolver DNS su Internet in genere richiedono i server di nomi solo una volta ogni due giorni e memorizzano nella cache le risposte.

I resolver DNS utilizzano ancora le vecchie impostazioni per il record

Se hai modificato le impostazioni in un record, ma il tuo traffico è ancora instradato alla risorsa precedente, come un server Web per il tuo sito Web, una possibile causa è che il DNS ha ancora le impostazioni precedenti memorizzate nella cache. Ogni record dispone di un TTL (time-to-live) che consente di specificare il periodo di tempo, in secondi, per cui il resolver DNS deve memorizzare nella cache le informazioni nel record, ad esempio l'indirizzo IP per un server Web. Fino a che non trascorre la quantità di tempo specificata dal TTL, i resolver DNS continueranno a restituire il valore precedente in risposta alle query DNS. Se si desidera sapere qual è il TTL per un record, eseguire la procedura seguente.

> **Note**
>
> Per i record di alias, il TTL è determinato dalla AWS risorsa verso cui il record indirizza il traffico. Per ulteriori informazioni, consulta Scelta tra record alias e non alias.

Per visualizzare il TTL per un record

1. Accedi a AWS Management Console e apri la console Route 53 all'indirizzo. https://console.aws.amazon.com/route53/
2. Nella pagina Hosted Zones (Zone ospitate), scegli il nome della zona ospitata che include il record.
3. Nell'elenco dei record, trova il record per cui desideri il valore TTL e controlla il valore della colonna TTL.

> **Note**
>
> Modificare il TTL ora non rende più rapida l'applicazione delle modifiche. I resolver DNS hanno già il valore memorizzato nella cache, e non ottengono la nuova impostazione fino a quando la quantità di tempo specificata dalla vecchia impostazione non sarà trascorsa.

Hai più di una zona ospitata con lo stesso nome e hai aggiornato quella che non è associata al dominio

Puoi creare più di una zona ospitata con lo stesso nome utilizzando lo stesso account o più account. Per specificare la zona ospitata utilizzata da Route 53 per instradare il traffico Internet per il dominio, ottieni i quattro server dei nomi di Route 53 per tale zona ospitata e aggiorna la registrazione del dominio per utilizzare tali server di nomi.

Se aggiungi, modifichi o elimini i record in una zona ospitata ma la registrazione del dominio utilizza i server di nomi per un'altra zona ospitata, le risposte di Route 53 alle query DNS non rifletteranno le modifiche. Per determinare se la registrazione del dominio utilizza i server di nomi per la zona ospitata in cui sono stati aggiornati i record, esegui le operazioni seguenti:

1. Determinare quali server di nomi sono associati alla registrazione del dominio. Per informazioni, consulta Aggiunta o modifica di server dei nomi o glue record.
2. Confronta i server di nomi ottenuti nella fase 1 con i server dei nomi assegnati da Route 53 alla zona ospitata in cui sono stati aggiornati i record. Per informazioni, consulta Ottenere i server di nomi per una zona ospitata pubblica.

Se i server di nomi per la registrazione del dominio non corrispondono ai server di nomi per la zona ospitata in cui sono stati aggiornati i record, sono disponibili due opzioni:

Modificare i record nella zona ospitata attualmente associata al dominio (scelta consigliata)

Prendi nota delle modifiche apportate nella zona ospitata che non è attualmente associata alla registrazione del dominio. Quindi passa alla zona ospitata associata alla registrazione del dominio e apporta le stesse modifiche. Questo è il metodo preferito perché le modifiche hanno effetto quasi immediatamente. Per ulteriori informazioni, consulta Modifica di record.

Aggiornare la registrazione del dominio per utilizzare server di nomi diversi

Modifica la registrazione del dominio per utilizzare i server di nomi nella zona ospitata aggiornata.

> **Important**
>
> Se modifichi i server di nomi associati alla registrazione del dominio, il dominio non sarà disponibile su Internet per un massimo di 2 giorni. Questo perché i resolver DNS in genere memorizzano nella cache i nomi dei server di nomi per 2 giorni. Per una panoramica del funzionamento del DNS, incluse le informazioni sulla memorizzazione nella cache del resolver, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Modificando i server di nomi associati alla registrazione del dominio, si sta essenzialmente modificando il servizio DNS per il dominio. Sono disponibili due opzioni, a seconda se il dominio è attualmente in uso:

- Se il dominio è in uso, consulta Rendere Route 53 il servizio DNS per un dominio in uso.
- Se il dominio è attualmente inattivo, esegui le seguenti attività:
  1. Ottenere i server di nomi per la zona ospitata che si desidera utilizzare per instradare il traffico al dominio. Per informazioni, consulta Ottenere i server di nomi per una zona ospitata pubblica.
  2. Nella zona ospitata per cui sono disponibili i server di nomi nella fase 1, verificare che il record NS utilizzi gli stessi quattro server di nomi. In caso contrario, aggiornare il record NS. Per informazioni, consulta Modifica di record.
  3. Aggiorna la registrazione del dominio per utilizzare i server di nomi ottenuti nella fase 1. Per informazioni, consulta Aggiunta o modifica di server dei nomi o glue record.

Il mio browser visualizza un errore "Server not found" (Server non trovato)

Se il browser visualizza un errore "Server not found" (Server non trovato) quando si tenta di accedere a un dominio (esempio.com) o a un sottodominio (www.esempio.com), ecco alcuni chiarimenti comuni.

Argomenti

Non hai creato un record per il nome di dominio o sottodominio

Se non crei un record per il dominio o sottodominio, DNS non sa dove instradare il traffico quando un utente immette tale nome in un browser. Per ulteriori informazioni, consulta Utilizzo dei record.

Hai creato un record ma hai specificato il valore errato

Quando crei un record, è facile specificare il valore sbagliato, ad esempio l'indirizzo IP di un server web o il nome di dominio CloudFront assegnato alla tua distribuzione web. Se il record esiste ma stai ancora ottenendo l'errore "Server not found" (Server non trovato), ti consigliamo di verificare che il valore sia corretto.

La risorsa a cui stai instradando il traffico non è disponibile

Se un record specifica una risorsa, ad esempio un server Web non disponibile, un browser restituisce un errore "Server not found" (Server non trovato). Ti consigliamo di verificare lo stato della risorsa a cui stai instradando il traffico.

Non riesco a instradare il traffico a un bucket Amazon S3 configurato per l'hosting di siti Web

Quando configuri un bucket Amazon S3 per l'hosting di siti Web, è necessario fornire al bucket lo stesso nome del record che si desidera utilizzare per instradare il traffico verso il bucket. Ad esempio,

se si desidera instradare il traffico per esempio.com a un bucket S3 configurato per l'hosting di siti Web, il nome del bucket deve essere esempio.com.

Se desideri indirizzare il traffico verso un bucket S3 configurato per l'hosting di siti Web ma il nome del bucket non compare nell'elenco Alias Target nella console Amazon Route 53, o se stai cercando di creare un record di alias a livello di codice e ricevi un InvalidInput errore dall'API Route 53, uno dei, oppure AWS SDKs, controlla quanto segue: AWS CLI AWS Tools for Windows PowerShell

- Il nome del bucket deve corrispondere esattamente al nome del record, ad esempio esempio.com o www.esempio.com.
- Il bucket S3 deve essere correttamente configurato per l'hosting di siti Web. Per ulteriori informazioni, consulta Hosting di un sito Web statico su Amazon S3 nella Guida per gli utenti di Amazon Simple Storage Service.

Mi è stato fatturata due volte la stessa zona ospitata

Non applichiamo addebiti se elimini una zona ospitata entro 12 ore dalla creazione. Dopo 12 ore, addebitiamo immediatamente la tariffa mensile standard per una zona ospitata. La tariffa mensile per una zona ospitata non è ripartita proporzionalmente per mesi parziali. (Lo stesso addebito si applica alla zona ospitata che creiamo automaticamente quando record un dominio.)

Se si crea una zona ospitata l'ultimo giorno del mese (ad esempio, il 31 gennaio), il costo per gennaio potrebbe apparire sulla fattura di febbraio, insieme al costo per febbraio. Tieni presente che Amazon Route 53 utilizza UTC come fuso orario per determinare quando è stata creata una zona ospitata.

Mi sono state addebitate più fatture per il mio dominio

Quando sottoscrivi un abbonamento, paghi una quota di registrazione, una commissione di trasferimento o una tassa di rinnovo con un costo iniziale, viene generata una fattura unica. Questa fattura rimane sulla console di fatturazione, anche se la transazione di pagamento non va a buon fine. La relativa voce di fatturazione viene mostrata come [x] Quantità nella sottosezione Registrar-Global della scheda Bill details by service della console di fatturazione.

Per visualizzare le fatture esentate, completa i seguenti passaggi:

Per visualizzare le fatture revocate sulla console di fatturazione

1. Accedi AWS Management Console e apri la console all'indirizzo. AWS Billing and Cost Management https://console.aws.amazon.com/costmanagement/
2. Nel riquadro di navigazione selezionare Bills (Fatture).
3. Scegli Fatture per visualizzare i dettagli di eventuali fatture non valide.

Per visualizzare i pagamenti e i rimborsi andati a buon fine sulla console di fatturazione, completa i seguenti passaggi:

Per confermare i pagamenti o i rimborsi che sono stati elaborati correttamente

1. Nel riquadro di navigazione, scegli Pagamenti.
2. Scegli la scheda Transazioni per visualizzare la tabella Transazioni per tutte le transazioni completate con AWS.

Il mio AWS account è chiuso o definitivamente e il mio dominio è registrato con Route 53

Se chiudi il tuo AWS account, o se il tuo account viene chiuso o chiuso definitivamente, i tuoi domini verranno sottoposti a una procedura di cancellazione:

1. Ti informeremo che il tuo account è chiuso e il tuo dominio verrà sospeso ogni giorno nei prossimi 5 giorni.
2. Una volta sospeso il dominio, si verificherà quanto segue:
   - Se il tuo registrar è Amazon Registrar, ti avviseremo che elimineremo il tuo dominio entro 30 giorni. Per ulteriori informazioni, consulta Ricerca del registrar e altre informazioni sul tuo dominio.
   - Se il tuo registrar è Gandi, ti avviseremo che rilasceremo il tuo dominio a Gandi quando il tuo account verrà chiuso definitivamente.
3. Dopo aver atteso 30 giorni, elimineremo tutti i domini registrati con Amazon Registrar nell'account e ti invieremo un aggiornamento.
4. Quando il tuo account verrà chiuso definitivamente, rilasceremo a Gandi tutti i domini registrati con Gandi nell'account.

Se riapri il tuo account durante il periodo in cui i domini possono essere recuperati, annulleremo la sospensione dei tuoi domini o ti informeremo che i tuoi domini sono stati eliminati ma potrebbero essere ripristinati. Per ulteriori informazioni, consulta Domini che è possibile registrare con Amazon Route 53.

> **Note**
>
> Una volta trascorsi 90 giorni dalla chiusura dell'account, non è più possibile riaprirlo. Per ulteriori informazioni, consulta Chiusura di un account nella guida alla gestione dell'account.AWS

Per ulteriori informazioni, consulta Contattare l' AWS assistenza per problemi relativi alla registrazione del dominio.

Intervalli di indirizzi IP di server Amazon Route 53

Amazon Web Services (AWS) pubblica i propri intervalli di indirizzi IP correnti in formato JSON. Se il firewall o i gruppi di sicurezza limitano il traffico in entrata in base agli indirizzi IP di origine, verifica che la configurazione consenta il traffico dall'intervallo di indirizzi IP valido.

Per visualizzare gli intervalli di indirizzi IP correnti per Route 53, scarica ip-ranges.json e cerca nel file i seguenti valori:

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

Per ulteriori informazioni sugli indirizzi IP per AWS le risorse, vedere Intervalli di indirizzi AWS IP in Riferimenti generali di Amazon Web Services.

Intervalli di indirizzi IP di name server di Route 53

`"service": "ROUTE53"`: questi intervalli di indirizzi IP vengono utilizzati dai name server di Route 53. Aggiungi questi intervalli all'elenco di intervalli di indirizzi IP, se utilizzi Route 53 come servizio DNS per uno o più domini e desideri utilizzare i comandi `dig` o `nslookup` per eseguire query sui server dei nomi di Route 53.

> **Note**
>
> Solo raramente modifichiamo gli indirizzi IP dei server di nomi; se è necessario modificare gli indirizzi IP, ti invieremo una notifica in anticipo.

Intervalli di indirizzi IP dei controlli dell'integrità di Route 53

`"service": "ROUTE53_HEALTHCHECKS"`: questi intervalli di indirizzi IP vengono utilizzati dai controlli dell'integrità di Route 53. Aggiungi questi intervalli all'elenco degli intervalli di indirizzi IP consentiti se utilizzi controlli dell'integrità di Route 53 per verificare lo stato delle risorse della rete.

> **Note**
>
> Raramente modifichiamo gli intervalli di indirizzi IP degli operatori sanitari; se abbiamo bisogno di modificare gli intervalli di indirizzi IP, ti avviseremo in anticipo.

Per ulteriori informazioni sugli indirizzi IP per i controlli dell'integrità, consulta Configurazione di regole di router e firewall per i controlli dell'integrità di Amazon Route 53.

Riferimento di elenchi di prefissi

Un elenco di prefissi è un set di una o più voci di blocco CIDR utilizzabile per configurare i gruppi di sicurezza. Il router e il firewall per le regole per l' EC2istanza Amazon devono consentire il traffico in entrata dagli indirizzi IP utilizzati dai controllori dello stato della Route 53. Un riferimento a un elenco di prefissi consente di semplificare la gestione dei blocchi CIDR nelle regole. Se utilizzi spesso lo stesso CIDRs per più regole, puoi gestirle CIDRs in un unico elenco di prefissi, anziché fare ripetutamente riferimento allo stesso CIDRs in ogni regola. Se hai bisogno di rimuovere un blocco CIDR, puoi rimuovere la relativa voce dall'elenco dei prefissi anziché rimuovere il CIDR da ogni regola interessata. Per maggiori informazioni sugli elenchi di prefissi in generale, consulta Raggruppare blocchi CIDR tramite elenchi di prefissi gestiti nella Guida dell'utente di Amazon VPC.

AWS-gli elenchi di prefissi gestiti sono insiemi di intervalli di indirizzi IP per i servizi. AWS AWS-gli elenchi di prefissi gestiti vengono creati e gestiti da AWS e possono essere utilizzati da chiunque disponga di un account. AWS Non è possibile creare, modificare, condividere o eliminare un elenco di prefissi AWS-managed.

Per ulteriori informazioni sugli elenchi di prefissi AWS-managed, consulta Work with AWS-managed prefix lists nella Amazon VPC User Guide.

Intervalli di indirizzi IP interni dei controlli dell'integrità di Route 53

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`: Route 53 utilizza questi intervalli di indirizzi IP solo internamente. Non è necessario aggiungere questi intervalli all'elenco degli intervalli consentiti.

Assegnazione di tag alle risorse di Amazon Route 53

Un tag è un'etichetta che assegni a una risorsa. AWS Ogni tag consiste di una chiave e di un valore, entrambi personalizzabili. Ad esempio, la chiave potrebbe essere "dominio" e il valore potrebbe essere "example.com". È possibile usare i tag per un'ampia gamma di scopi; un uso comune è di suddividere in categorie e monitorare i costi di Amazon Route 53. Quando applichi tag alle zone ospitate, ai domini e ai controlli sanitari di Route 53, AWS genera un rapporto sull'allocazione dei costi come file con valori separati da virgole (CSV) con l'utilizzo e i costi aggregati dai tag. Puoi applicare i tag che rappresentano categorie di business (come centri di costo, nomi di applicazioni o proprietari) per organizzare i costi tra più servizi. Per ulteriori informazioni sull'utilizzo dei tag per l'allocazione dei costi, consultare Uso dei tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing.

Per facilità d'uso e risultati ottimali, utilizza Tag Editor in the AWS Management Console, che fornisce un modo centralizzato e unificato per creare e gestire i tag. Per ulteriori informazioni, consultare Utilizzo dell'editor di tag in Nozioni di base sulla AWS Management Console. Per applicare tag ad alcune risorse è possibile utilizzare anche la console Route 53:

- Controlli dell'integrità: per ulteriori informazioni, consultare Denominazione e tagging di controlli dell'integrità.
- Endpoint in entrata di Route 53 Resolver: per ulteriori informazioni, consultare Valori specificati durante la creazione o la modifica di endpoint in entrata.
- Endpoint in uscita di Resolver: per ulteriori informazioni, consultare Valori specificati durante la creazione o la modifica degli endpoint in uscita.
- Regole di Resolver: per ulteriori informazioni, consultare Valori specificati durante la creazione o la modifica delle regole.
- Zone ospitate: per maggiori informazioni, consultare Utilizzo delle zone ospitate.

> **Note**
>
> I costi per gli endpoint Resolver vengono assegnati per interfaccia di rete Resolver. Poiché attualmente non è possibile etichettare le interfacce di rete Resolver, l'allocazione dei costi basata su tag non è attualmente supportata per gli endpoint Resolver. Per informazioni sui prezzi di Resolver, consultare Prezzi di Amazon Route 53.

Inoltre, è possibile applicare tag a risorse utilizzando l'API Route 53. Per ulteriori informazioni, consultare le azioni correlate ai tag nell'argomento Operazioni API Route 53 per funzione nella Documentazione di riferimento dell'API di Amazon Route 53.

Tutorial

Questa sezione tratta i seguenti tutorial:

Utilizzo di Route 53 come servizio DNS per i sottodomini

Scopri come utilizzare Route 53 come servizio DNS per un sottodominio nuovo o esistente continuando a utilizzare un altro servizio DNS per il dominio principale.

Passaggio al routing basato sulla latenza

Scopri come migrare gradualmente dal routing standard al routing basato sulla latenza in Route 53, indirizzando gli utenti verso l'endpoint con la latenza più bassa disponibile. AWS

Combina record ponderati e di latenza per una transizione fluida e a basso rischio con funzionalità complete di controllo e rollback.

Aggiungere un'altra regione al routing basato sulla latenza

Espandi la configurazione del routing basato sulla latenza aggiungendo una nuova AWS regione e spostando gradualmente il traffico verso la nuova regione.

Instradamento del traffico verso più EC2 istanze Amazon in una regione

Usa una combinazione di latenza e record ponderati per indirizzare il traffico verso più EC2 istanze Amazon all'interno di una specifica. Regione AWS

Gestione di oltre 100 record ponderati

Scopri come indirizzare il traffico verso più di 100 endpoint creando un albero di record di alias ponderati e record ponderati.

Ponderazione delle risposte multi-record con tolleranza agli errori

Scopri come ponderare le risposte DNS che contengono più record, garantendo la tolleranza agli errori e il bilanciamento del carico su più endpoint.

Questi tutorial coprono vari casi d'uso e scenari, aiutandoti a sfruttare efficacemente le politiche di routing, i record ponderati e il routing basato sulla latenza di Route 53 per ottimizzare la gestione del DNS e il routing del traffico.

Argomenti

Utilizzo di Amazon Route 53 come servizio DNS per i sottodomini senza migrare il dominio padre

Amazon Route 53 offre flessibilità nella gestione del DNS per i sottodomini, consentendoti di sfruttare le sue funzionalità senza la necessità di migrare l'intero dominio principale.

Puoi creare un nuovo sottodominio o migrarne uno esistente su Route 53, mantenendo il dominio principale ospitato presso un altro provider di servizi DNS.

Creazione di un nuovo sottodominio con Route 53:

1. Crea una zona ospitata per il nuovo sottodominio.
2. Aggiungi i record DNS desiderati (ad esempio, A, CNAME, MX) per il sottodominio alla zona ospitata.
3. Ottieni i name server Route 53 assegnati alla zona ospitata.
4. Aggiorna la configurazione DNS del dominio principale aggiungendo i record NS (Name Server) per il sottodominio, che puntano ai name server Route 53.

Migrazione di un sottodominio esistente su Route 53:

1. Creare una zona ospitata per il sottodominio.
2. Ottieni la configurazione DNS corrente per il sottodominio dal tuo provider di servizi DNS esistente.
3. Aggiungi i record DNS corrispondenti alla zona ospitata.
4. Ottieni i name server Route 53 assegnati alla zona ospitata.
5. Aggiorna la configurazione DNS del dominio principale aggiungendo i record NS per il sottodominio, che puntano ai name server Route 53.

Seguendo questi passaggi, puoi sfruttare le funzionalità avanzate di Route 53, come i controlli di integrità, le politiche di routing e la gestione del flusso di traffico, per i tuoi sottodomini mantenendo al contempo la configurazione DNS del dominio principale con il tuo provider esistente.

Argomenti

Creazione di un sottodominio che usa Amazon Route 53 come servizio DNS senza migrazione del dominio padre

Crea un sottodominio che utilizza Amazon Route 53 come servizio DNS senza migrare il dominio padre da un altro servizio DNS.

Il processo ha i seguenti passaggi di base:

1. Determinare se occorre utilizzare questa procedura.
2. Crea una zona ospitata Route 53 per il sottodominio.
3. Aggiungi record per il sottodominio alla zona ospitata Route 53.
4. Solo API: conferma che le modifiche sono state estese a tutti i server DNS di Route 53.

> **Note**
>
> Attualmente, l'unico modo per verificare che le modifiche si siano propagate consiste nell'utilizzare l'azione GetChangeAPI. In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

5. Aggiornare il servizio DNS per il dominio padre aggiungendo i record dei server dei nomi per il sottodominio.

Individuazione delle procedure da usare per la creazione di un sottodominio

Le procedure in questo argomento illustrano come eseguire un'operazione insolita. Se stai già utilizzando Route 53 come servizio DNS per il tuo dominio e desideri semplicemente indirizzare il

traffico da un sottodominio, come www.example.com, verso le tue risorse, ad esempio un server Web in esecuzione su un'istanza, vedi. EC2 Routing del traffico per sottodomini

Utilizza questa procedura solo se stai utilizzando un altro servizio DNS per un dominio, ad esempio esempio.com, e desideri iniziare a utilizzare Route 53 come servizio DNS per un nuovo sottodominio di quel dominio, ad esempio www.esempio.com.

Creazione di una zona ospitata per il nuovo sottodominio

Se desideri utilizzare Amazon Route 53 come servizio DNS per un nuovo sottodominio senza migrare il dominio padre, inizia creando una zona ospitata per il sottodominio. Route 53 memorizza informazioni sul tuo sottodominio nella hosted zone.

Per informazioni su come creare una zona ospitata utilizzando la console Route 53, consulta Creazione di una zona ospitata pubblica.

Creazione di record

Puoi creare i record utilizzando la console Amazon Route 53 o l'API Route 53. I record che crei in Route 53 diventeranno i record che DNS usa dopo che deleghi la responsabilità per il sottodominio a Route 53, come spiegato in Aggiornamento del servizio DNS con record di server dei nomi per il sottodominio, in un secondo momento.

> **Important**
>
> Non creare ulteriori record di server di nomi (NS) o origine di autorità (SOA) nella zona ospitata di Route 53 e non eliminare i record SOA e NS esistenti.

Per creare i record tramite la console Route 53, consulta Utilizzo dei record. Per creare i record tramite l'API Route 53, consulta `ChangeResourceRecordSets`. Per ulteriori informazioni, ChangeResourceRecordSetsconsulta Amazon Route 53 API Reference.

Verifica dello stato delle modifiche (solo API)

La creazione di una nuova zona ospitata e la modifica dei record richiedono tempo per la propagazione ai server DNS di Route 53. Se in passato ChangeResourceRecordSetscreavi i tuoi record, puoi utilizzare l'`GetChange`azione per determinare se le modifiche si sono propagate. (`ChangeResourceRecordSets`restituisce un valore per`ChangeId`, che è possibile includere in una

`GetChange` richiesta successiva. `ChangeId`non è disponibile se i record sono stati creati utilizzando la console.) Per ulteriori informazioni, consulta GET GetChange nel riferimento alle API di Amazon Route 53.

> **Note**
>
> In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Aggiornamento del servizio DNS con record di server dei nomi per il sottodominio

Dopo che le modifiche ai record Amazon Route 53 sono state propagate (consulta Verifica dello stato delle modifiche (solo API)), aggiorna il servizio DNS per il dominio padre aggiungendo record NS per il sottodominio. Questo è noto come delegare la responsabilità per il sottodominio a Route 53. Ad esempio, se il dominio padre esempio.com è ospitato con un altro servizio DNS ed è stato creato il sottodominio test.esempio.com in Route 53, devi aggiornare il servizio DNS per esempio.com con i nuovi record NS per test.esempio.com.

Esegui la seguente procedura.

1. Utilizzando il metodo fornito dal servizio DNS, esegui il backup dei file di zona per il dominio padre.
2. Nella console Route 53, ottieni i server dei nomi per la tua zona ospitata Route 53

   a. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
   b. Nel pannello di navigazione, scegli Zone ospitate.
   c. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata, quindi seleziona Visualizza dettagli.
   d. Nella pagina dei dettagli della zona ospitata, scegli Dettagli della zona ospitata.
   e. Prendi nota dei quattro server indicati per Server dei nomi.

   In alternativa, puoi utilizzare l'operazione `GetHostedZone`. Per ulteriori informazioni, GetHostedZoneconsulta Amazon Route 53 API Reference.
3. Utilizzando il metodo fornito dal servizio DNS del dominio padre, aggiungi record NS per il sottodominio al file di zona per il dominio padre. In questi record NS, specifica i quattro server dei nomi di Route 53 che sono associati alla zona ospitata creata nella Fase 1.

> **Important**
>
> Non aggiungere un record di origine di autorità (SOA) per il file di zona per il dominio padre. Poiché il sottodominio utilizzerà Route 53, il servizio DNS per il dominio padre non è l'autorità per il sottodominio.
> Se il servizio DNS ha aggiunto automaticamente un record SOA per il sottodominio, elimina il record per il sottodominio. Tuttavia, non eliminare il record SOA per il dominio padre.

Migrazione del servizio DNS per un sottodominio ad Amazon Route 53 senza migrazione del dominio padre

Puoi eseguire la migrazione di un sottodominio per utilizzare Amazon Route 53 come servizio DNS senza migrare il dominio padre da un altro servizio DNS.

Il processo ha i seguenti passaggi di base:

1. Determinare se occorre utilizzare questa procedura.
2. Crea una zona ospitata Route 53 per il sottodominio.
3. Ottenere l'attuale configurazione DNS dal fornitore di servizi DNS per il dominio padre.
4. Aggiungi record per il sottodominio alla zona ospitata Route 53.
5. Solo API: conferma che le modifiche sono state estese a tutti i server DNS di Route 53.

   > **Note**
   >
   > Attualmente, l'unico modo per verificare che le modifiche si siano propagate consiste nell'utilizzare l'azione GetChangeAPI. In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

6. Aggiornare la configurazione DNS con il fornitore di servizi DNS per il dominio padre aggiungendo record del server dei nomi per il sottodominio.

Individuazione delle procedure da usare per la creazione di un sottodominio

Le procedure in questo argomento illustrano come eseguire un'operazione insolita. Se stai già utilizzando Route 53 come servizio DNS per il tuo dominio e desideri semplicemente indirizzare il

traffico da un sottodominio, come www.example.com, verso le tue risorse, ad esempio un server Web in esecuzione su un'istanza, vedi. EC2 Routing del traffico per sottodomini

Utilizza questa procedura solo se stai utilizzando un altro servizio DNS per un dominio, ad esempio esempio.com, e desideri iniziare a utilizzare Route 53 come servizio DNS per un sottodominio esistente di quel dominio, ad esempio www.esempio.com.

Creazione di una zona ospitata per il sottodominio

Se desideri migrare un sottodominio da un altro servizio DNS ad Amazon Route 53 ma non desideri migrare il dominio padre, inizia creando una zona ospitata per il sottodominio. Route 53 memorizza informazioni sul tuo sottodominio nella hosted zone.

Per informazioni su come creare una zona ospitata utilizzando la console Route 53, consulta Creazione di una zona ospitata pubblica.

Ottenere l'attuale configurazione DNS dal fornitore di servizi DNS

Per semplificare il processo di migrazione di un sottodominio esistente a Route 53, ottieni l'attuale configurazione DNS per il dominio dal provider di servizi DNS, che attualmente esegue manutenzione sul dominio. Puoi utilizzare queste informazioni come base per configurare Route 53 come servizio DNS per il sottodominio.

Ciò che chiedi e il formato che ottieni in varia in base all'azienda che utilizzi come fornitore di servizi DNS. Idealmente, riceverai un file di zona, che contiene informazioni su tutti i record nella configurazione corrente. (I record indicano al DNS come desideri che venga indirizzato il traffico per i tuoi domini e sottodomini. Ad esempio, quando qualcuno inserisce il tuo nome di dominio in un browser Web, desideri che il traffico venga indirizzato a un server Web nel tuo data center, a un' EC2 istanza Amazon, a una CloudFront distribuzione o a qualche altra posizione?) Se puoi ottenere un file di zona dal tuo attuale provider di servizi DNS, puoi modificare il file di zona per rimuovere i record per cui non desideri eseguire la migrazione a Amazon Route 53. Quindi puoi importare i record rimanenti nella tua zona ospitata Route 53, il che semplifica notevolmente il processo. Prova a chiedere all'assistenza clienti del tuo attuale fornitore di servizi DNS come ottenere un file di zona o un elenco di record.

Creazione di record

Utilizzando i record ottenuti dal provider di servizi DNS corrente come punto di partenza, crea i record corrispondenti nella zona ospitata di Amazon Route 53 creata per il sottodominio. I record che crei in

Route 53 diventeranno i record che DNS usa dopo che deleghi la responsabilità per il sottodominio a Route 53, come spiegato in Aggiornamento del servizio DNS con record di server dei nomi per il sottodominio, in un secondo momento.

> **Important**
>
> Non creare ulteriori record di server di nomi (NS) o origine di autorità (SOA) nella zona ospitata di Route 53 e non eliminare i record SOA e NS esistenti.

Per creare i record tramite la console Route 53, consulta Utilizzo dei record. Per creare i record tramite l'API Route 53, consulta `ChangeResourceRecordSets`. Per ulteriori informazioni, ChangeResourceRecordSetsconsulta Amazon Route 53 API Reference.

Verifica dello stato delle modifiche (solo API)

La creazione di una nuova zona ospitata e la modifica dei record richiedono tempo per la propagazione ai server DNS di Route 53. Se in passato ChangeResourceRecordSetscreavi i tuoi record, puoi utilizzare l'`GetChange`azione per determinare se le modifiche si sono propagate. (`ChangeResourceRecordSets`restituisce un valore per`ChangeId`, che è possibile includere in una `GetChange` richiesta successiva. `ChangeId`non è disponibile se i record sono stati creati utilizzando la console.) Per ulteriori informazioni, consulta GET GetChange nel riferimento alle API di Amazon Route 53.

> **Note**
>
> In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi.

Aggiornamento del servizio DNS con record di server dei nomi per il sottodominio

Dopo che le modifiche ai record Amazon Route 53 sono state propagate (consulta Verifica dello stato delle modifiche (solo API)), aggiorna il servizio DNS per il dominio padre aggiungendo record NS per il sottodominio. Questo è noto come delegare la responsabilità per il sottodominio a Route 53. Ad esempio, supponiamo che il dominio padre esempio.com sia ospitato con un altro servizio DNS e che tu stia migrando il sottodominio test.esempio.com a Route 53. Devi creare una zona ospitata per test.esempio.com e aggiornare il servizio DNS per esempio.com con il record NS che Route 53 ha assegnato alla nuova zona ospitata per test.esempio.com.

Esegui la seguente procedura.

1. Utilizzando il metodo fornito dal servizio DNS, esegui il backup dei file di zona per il dominio padre.
2. Se il precedente fornitore di servizi DNS per il dominio dispone di un metodo per modificare le impostazioni di TTL per i propri server di nomi, ti consigliamo di modificare le impostazioni su 900 secondi. Questo limita il tempo durante il quale le richieste client tentano di risolvere i nomi di dominio utilizzando server di nomi obsoleti. Se l'attuale TTL è 172800 secondi (due giorni), che è un'impostazione di default comune, devi comunque attendere due giorni affinché resolver e client smettono di memorizzare nella cache i record DNS utilizzando il TTL precedente. Una volta scadute le impostazioni di TTL, potrai eliminare in modo sicuro i record che sono stati archiviati presso il provider precedente e apportare le modifiche solo a Route 53.
3. Nella console Route 53, ottieni i server dei nomi per la tua zona ospitata Route 53

   a. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

   b. Nel pannello di navigazione, scegli Zone ospitate.

   c. Nella pagina Zone ospitate, scegli il pulsante di opzione (non il nome) per la zona ospitata, quindi seleziona Visualizza dettagli.

   d. Nella pagina dei dettagli della zona ospitata, scegli Dettagli della zona ospitata.

   e. Prendi nota dei quattro server indicati per Server dei nomi.

   In alternativa, puoi utilizzare l'operazione `GetHostedZone`. Per ulteriori informazioni, GetHostedZoneconsulta Amazon Route 53 API Reference.
4. Utilizzando il metodo fornito dal servizio DNS del dominio padre, aggiungi record NS per il sottodominio al file di zona per il dominio padre. Dai ai record NS lo stesso nome del sottodominio. Per i valori nei record NS, specifica i quattro server dei nomi di Route 53 associati alla zona ospitata creata nella Fase 2. Servizi DNS diversi usano una terminologia differente. Potrebbe essere necessario contattare il supporto tecnico del servizio DNS per ulteriori informazioni su come eseguire questa operazione.

   > **Important**
   >
   > Non aggiungere un record di origine di autorità (SOA) per il file di zona per il dominio padre. Poiché il sottodominio utilizzerà Route 53, il servizio DNS per il dominio padre non è l'autorità per il sottodominio.

Se il servizio DNS ha aggiunto automaticamente un record SOA per il sottodominio, elimina il record per il sottodominio. Tuttavia, non eliminare il record SOA per il dominio padre.

A seconda delle impostazioni di TTL per i server di nomi per il dominio padre, la propagazione delle modifiche apportate ai resolver DNS può richiedere 48 ore o più. Durante tale periodo, i resolver DNS possono ancora rispondere a richieste con i server di nomi per il servizio DNS del dominio padre. Inoltre, i computer client potrebbero continuare a disporre del nome del server precedente per il sottodominio nella cache.

5. Dopo che le impostazioni TTL del registrar per il dominio scadono (vedi Fase 2), eliminare i seguenti record dal file di zona per il dominio padre:

   - I record aggiunti a Route 53 come descritto in Creazione di record.
   - I record NS del servizio DNS. Una volta completata l'eliminazione di record NS, gli unici record NS nel file di zona saranno quelli creati nella Fase 4.

Transitioning to latency-based routing in Amazon Route 53

Con il routing basato sulla latenza, Amazon Route 53 può indirizzare gli utenti verso l'endpoint con la latenza più bassa disponibile. AWS Ad esempio, potresti associare un nome DNS a un ELB Classic, Application o Network Load Balancer oppure a istanze EC2 Amazon o indirizzi IP elastici ospitati nelle regioni Stati Uniti orientali (Ohio) ed Europa (Irlanda). `www.example.com` I server DNS di Route 53 decidono, in base alle condizioni di rete delle ultime due settimane, quali istanze in quali regioni devono servire particolari utenti. Un utente a Londra potrebbe essere indirizzato all'istanza Europa (Irlanda), un utente a Chicago potrebbe essere indirizzato all'istanza Stati Uniti orientali (Ohio) e così via. Route 53 supporta il routing basato sulla latenza per record A, AAAA, TXT e CNAME, nonché alias a record A e AAAA.

> **Note**
>
> I dati sulla latenza tra utenti e risorse si basano interamente sul traffico tra utenti e data center. AWS Se non utilizzi risorse in una AWS regione, la latenza effettiva tra gli utenti e le risorse può variare in modo significativo rispetto ai dati di AWS latenza. Questo vale anche se le tue risorse si trovano nella stessa città di una AWS regione.

Per una transizione fluida, puoi combinare record ponderati e di latenza per migrare gradualmente da routing standard a routing basato sulla latenza con il controllo completo e funzionalità di rollback in ogni fase. Consideriamo un esempio in cui `www.example.com` è attualmente ospitato su un' EC2 istanza Amazon nella regione Stati Uniti orientali (Ohio). L'istanza ha l'indirizzo IP elastico (EIP) `W.W.W.W`. Supponiamo di voler continuare a indirizzare il traffico verso la regione Stati Uniti orientali (Ohio), ove applicabile, iniziando anche a indirizzare gli utenti verso EC2 istanze Amazon aggiuntive nella regione Stati Uniti occidentali (California settentrionale) (IP elasticoX.X.X.X) e nella regione Europa (Irlanda) (IP elastico). `Y.Y.Y.Y` La zona ospitata di Route 53 `example.com` dispone già di un record per `www.example.com` che ha un Tipo A e un Valore(un indirizzo IP) pari a `W.W.W.W`.

Una volta terminato con il seguente esempio, avrai due record alias ponderati:

- Convertirai il record esistente per `www.example.com` in un record di alias ponderato che continua a indirizzare la maggior parte del traffico verso l' EC2 istanza Amazon esistente nella regione Stati Uniti orientali (Ohio).
- Puoi creare un altro record alias ponderato che inizialmente direziona solo una piccola porzione di traffico verso i record di latenza, che instradano il traffico verso le tre regioni.

Aggiornando i pesi di questi record di alias ponderati, puoi passare gradualmente dal routing del traffico solo verso la regione degli Stati Uniti orientali (Ohio) al routing del traffico verso tutte e tre le regioni in cui sono presenti istanze Amazon. EC2

Come passare a un routing basato sulla latenza

1. Creare una copia del record per `www.example.com`, ma utilizzare un nuovo nome di dominio, ad esempio `copy-www.example.com`. Assegnare al nuovo record lo stesso Type (Tipo) (A) e Value (Valore) (`W.W.W.W`) del record per `www.example.com`.
2. Aggiornare il record A esistente per `www.example.com` per renderlo un record alias ponderato:

   - Per Valore/instradamento traffico a, scegli Alias a un altro record in questa zona ospitata e specifica `copy-www.example.com`.
   - Per Peso, specifica 100.

   Una volta completato l'aggiornamento, Route 53 continuerà a usare questo record per indirizzare tutto il traffico alla risorsa che dispone di un indirizzo IP di `W.W.W.W`.
3. Crea un record di latenza per ciascuna delle tue EC2 istanze Amazon, ad esempio:

- Stati Uniti orientali (Ohio), indirizzo IP elastico `W.W.W.W`
- Stati Uniti occidentali (California settentrionale), indirizzo IP elastico `X.X.X.X`
- Europa (Irlanda), indirizzo IP elastico `Y.Y.Y.Y`

Assegnare a tutti i record di latenza lo stesso nome di dominio, ad esempio, `www-lbr.example.com` e lo stesso tipo, A.

Al termine della creazione dei record di latenza, Route 53 continuerà a instradare il traffico usando il record che hai aggiornato nella fase 2.

Puoi usare `www-lbr.example.com` per eseguire il testing di convalida, per esempio, per assicurare che ciascun endpoint possa accettare richieste.

4. Aggiungiamo ora il record di `www-lbr.example.com` latenza al record `www.example.com` ponderato e iniziamo a indirizzare il traffico limitato verso le istanze Amazon corrispondenti. EC2 Ciò significa che l' EC2 istanza Amazon nella regione Stati Uniti orientali (Ohio) riceverà traffico da entrambi i record ponderati.

   Creare un altro record alias ponderato per `www.example.com`:

   - Per Valore/instradamento traffico a, scegli Alias a un altro record in questa zona ospitata e specifica `www-lbr.example.com.`
   - Per Peso, specifica 1.

   Al termine e sincronizzate le modifiche con i server Route 53, Route 53 inizierà a indirizzare una piccola parte del traffico (1/101) verso EC2 le istanze Amazon per le quali hai creato i record di latenza nella Fase 3.

5. Mentre acquisisci sicurezza sul fatto che i tuoi endpoint vengano adeguatamente scalati per il traffico in entrata, regola i pesi di conseguenza. Ad esempio, se desidera che il 10% delle tue richieste siano basate sul routing basato sulla latenza, modifica il peso su 90 e 10 rispettivamente.

Per ulteriori informazioni sulla creazione di record di latenza, consulta Creazione di record utilizzando la console Amazon Route 53.

Aggiunta di un'altra regione al routing basato sulla latenza in Amazon Route 53

Se stai utilizzando il routing basato sulla latenza e desideri aggiungere un'istanza a una nuova regione, puoi spostare gradualmente il traffico verso la nuova regione nello stesso modo in cui viene spostato progressivamente il traffico al routing basato sulla latenza in Transitioning to latency-based routing in Amazon Route 53.

Ad esempio, supponiamo di utilizzare il routing basato sulla latenza per `www.example.com` indirizzare il traffico e di voler aggiungere un' EC2 istanza Amazon in Asia Pacifico (Tokyo) alle istanze negli Stati Uniti orientali (Ohio), Stati Uniti occidentali (California settentrionale) ed Europa (Irlanda). L'esempio di procedura seguente illustra un modo in cui è possibile aggiungere un'istanza in un'altra regione.

Per questo esempio, la zona ospitata Amazon Route 53 per `example.com` ha già un alias ponderato per `www.example.com` che instrada il traffico ai record basati sulla latenza per `www-lbr.example.com`:

- Stati Uniti orientali (Ohio), indirizzo IP elastico `W.W.W.W`
- Stati Uniti occidentali (California settentrionale), indirizzo IP elastico `X.X.X.X`
- Europa (Irlanda), indirizzo IP elastico `Y.Y.Y.Y`

Il record alias ponderato ha un peso di 100. Dopo essere passato al routing basato sulla latenza, presupponi che elimini l'altro record ponderato utilizzato per la transizione.

Come aggiungere un'altra regione al routing basato sulla latenza in Route 53

1. Creare quattro nuovi record basati sulla latenza che includono le tre regioni originali e la nuova regione in cui desideri iniziare a instradare il traffico.
   - Stati Uniti orientali (Ohio), indirizzo IP elastico `W.W.W.W`
   - Stati Uniti occidentali (California settentrionale), indirizzo IP elastico `X.X.X.X`
   - Europa (Irlanda), indirizzo IP elastico `Y.Y.Y.Y`
   - Asia Pacifico (Tokyo), indirizzo IP elastico `Z.Z.Z.Z`

Assegnare a tutti i record di latenza lo stesso nuovo nome di dominio, ad esempio, `www-lbr-2012-04-30.example.com` e lo stesso tipo, A.

Al termine della creazione dei record di latenza, Route 53 continuerà a instradare il traffico usando il record alias ponderato (`www.example.com`) e i record di latenza (`www-lbr.example.com`) originali.

Puoi usare i record `www-lbr-2012-04-30.example.com` per eseguire il testing di convalida, per esempio, per assicurare che ciascun endpoint possa accettare richieste.

2. Creare un record alias ponderato per i nuovi record di latenza:

   - Per il nome di dominio, specifica il nome per il record alias ponderati esistente, `www.example.com`.
   - Per Valore/instradamento traffico a, scegli Alias a un altro record in questa zona ospitata e specifica `www-lbr-2012-04-30.example.com`.
   - Per Peso, specifica 1.

   Al termine, Route 53 inizierà a indirizzare una piccola parte del traffico (1/101) verso EC2 le istanze Amazon per le quali hai creato i record di `www-lbr-2012-04-30.example.com` latenza nella Fase 1. Il resto del traffico continuerà a essere indirizzato ai record di `www-lbr.example.com` latenza, che non includono l' EC2 istanza Amazon nella regione Asia Pacifico (Tokyo).

3. Mentre acquisisci sicurezza sul fatto che i tuoi endpoint vengano adeguatamente scalati per il traffico in entrata, regola i pesi di conseguenza. Ad esempio, se desideri che il 10% delle tue richieste vengano instradate ai record di latenza che includono la regione di Tokyo, modifica il peso per `www-lbr.example.com` da 100 a 90 e il peso per `www-lbr-2012-04-30.example.com` da 1 a 10.

Per ulteriori informazioni sulla creazione di record, consulta Creazione di record utilizzando la console Amazon Route 53.

Utilizzo della latenza e dei record ponderati in Amazon Route 53 per indirizzare il traffico verso più EC2 istanze Amazon in una regione

Se la tua applicazione è in esecuzione su EC2 istanze Amazon in due o più EC2 regioni Amazon e se disponi di più di un' EC2 istanza Amazon in una o più regioni, puoi utilizzare il routing basato sulla latenza per indirizzare il traffico verso la regione corretta e quindi utilizzare record ponderati per instradare il traffico verso le istanze all'interno della regione in base ai pesi specificati.

Ad esempio, supponiamo di avere tre EC2 istanze Amazon con indirizzi IP elastici nella regione Stati Uniti orientali (Ohio) e di voler distribuire le richieste su tutte e tre in IPs modo uniforme per gli utenti per i quali Stati Uniti orientali (Ohio) è la regione appropriata. Una sola EC2 istanza Amazon è sufficiente nelle altre regioni, sebbene sia possibile applicare la stessa tecnica a più regioni contemporaneamente.

Utilizzare la latenza e i record ponderati in Amazon Route 53 per indirizzare il traffico verso più EC2 istanze Amazon in una regione

1. Crea un gruppo di record ponderati per le EC2 istanze Amazon nella regione. Tieni presente quanto segue:

   - Assegna a ogni record ponderato lo stesso valore per Nome record (ad esempio, `us-east.example.com`) e Tipo di record.
   - Per Valore/instradamento traffico a, scegli Indirizzo IP o un altro valore a seconda del tipo di record e specifica il valore di uno degli indirizzi IP elastici.
   - Se desideri ponderare equamente EC2 le istanze Amazon, specifica lo stesso valore per Weight.
   - Specifica un valore univoco per Set ID (Imposta ID) per ogni record.

   Per ulteriori informazioni sui record ponderati, consulta Routing ponderato.
2. Se hai più EC2 istanze Amazon in altre regioni, ripeti il passaggio 1 per le altre regioni. Specificare un valore diverso per Name (Nome) in ciascuna regione.
3. Per ogni regione in cui hai più EC2 istanze Amazon (ad esempio, Stati Uniti orientali (Ohio)), crea un record di alias di latenza. Per Valore/instradamento traffico a, scegli Alias a un altro record in questa zona ospitata e specifica il valore del campo Nome record (ad esempio, `us-east.example.com`) che è stato assegnato ai record ponderati in tale regione.

4. Per ogni regione in cui hai un' EC2 istanza Amazon, crea un record di latenza. Per il valore di Nome record, specifica lo stesso valore specificato per i record alias di latenza di record creati nella Fase 3. Per il traffico Value/Route verso, scegli l'indirizzo IP o un altro valore a seconda del tipo di record e specifica l'indirizzo IP elastico dell' EC2 istanza Amazon in quella regione.

   Per ulteriori informazioni sull'aggiunta di record di alias alle EC2 istanze Amazon, consulta Instradamento del traffico verso un'istanza Amazon EC2

Per ulteriori informazioni sulla creazione di record, consulta Creazione di record utilizzando la console Amazon Route 53.

Gestione di più di 100 record ponderati in Amazon Route 53

Amazon Route 53 consente di configurare i record ponderati. Per un determinato nome e tipo (ad esempio `www.example.com`, tipo A), è possibile configurare un massimo di 100 risposte alternative, ognuna con il proprio peso. Durante la risposta alle query per `www.example.com`, i server DNS di Route 53 selezionano una risposta random ponderata da restituire ai resolver DNS. Il valore di un record ponderato che ha un peso di 2 viene restituito, in media, due volte più spesso del valore di un record ponderato che ha un peso di 1.

Se hai bisogno di indirizzare il traffico verso più di 100 endpoint, un modo per farlo è di utilizzare una struttura di record alias ponderati e record ponderati. Ad esempio, il primo "livello" della struttura potrebbe contenere fino a 100 record alias ponderati, ciascuno dei quali può, a sua volta, puntare fino a un massimo di 100 record ponderati. Route 53 consente fino a tre livelli di conversione, che consentono di gestire fino a 1.000.000 endpoint ponderati univoci.

Una semplice struttura a due livelli può essere simile a questa:

Record di alias ponderati

- Alias `www.example.com` a `www-a.example.com` con un peso di 1
- Alias `www.example.com` a `www-b.example.com` con un peso di 1

Record ponderati

- `www-a.example.com`, tipo A, valore 192.0.2.1, peso 1
- `www-a.example.com`, tipo A, valore 192.0.2.2, peso 1

- `www-b.example.com`, tipo A, valore 192.0.2.3, peso 1
- `www-b.example.com`, tipo A, valore 192.0.2.4, peso 1

Per ulteriori informazioni sulla creazione di record, consulta Utilizzo dei record.

Ponderazione di risposte multi-record con tolleranza ai guasti in Amazon Route 53

> **Note**
>
> I record che utilizzano la policy di routing di risposta multivalore si comportano in modo analogo alla configurazione documentata in questo tutorial. La differenza principale è che la configurazione del tutorial consente di specificare un peso, che può essere utile quando i tuoi endpoint hanno capacità diverse. Per ulteriori informazioni, consulta Routing di risposta multivalore.

Un record ponderato di Amazon Route 53 può essere associato a un solo record, ovvero una combinazione di un nome (ad esempio, `example.com`) e un tipo di record (ad esempio, A). Ma è spesso auspicabile pesare risposte DNS che contengono più record.

Ad esempio, potresti avere otto EC2 istanze Amazon o endpoint Elastic IP per un servizio. Se il client di quel servizio supportano i nuovi tentativi di connessione (come tutti i browser più comuni), fornire più indirizzi IP nelle risposte DNS dà ai client endpoint alternativi in caso di errore di un endpoint particolare. Puoi persino proteggerti dal guasto di una zona di disponibilità se configuri le risposte in modo che contengano una combinazione di IPs ospitate in due o più zone di disponibilità.

Le risposte multi-record sono utili anche quando un numero elevato di client mobili (per esempio, applicazioni Web mobili) condividono un piccolo set di cache DNS. In questo caso, le risposte multi-record consentono ai client di indirizzare le richieste ai vari endpoint anche se ricevono una comune risposta DNS dalla cache condivisa.

Questi tipi di risposte multi-record possono essere ottenute utilizzando una combinazione di record e record alias ponderati. È possibile raggruppare otto endpoint in due distinti di set di record contenenti quattro indirizzi IP ciascuno:

`endpoint-a.example.com`, tipo A, con i seguenti valori:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, tipo A, con i seguenti valori:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

È quindi possibile creare un record alias ponderato che punti a ciascun gruppo:

- Alias `www.example.com` a `endpoint-a.example.com`, tipo A, peso di 1
- Alias `www.example.com` a `endpoint-b.example.com`, tipo A, peso di 1

Per ulteriori informazioni sulla creazione di record, consulta Utilizzo dei record.

Best practice per Amazon Route 53

Questa sezione fornisce le best practice per vari componenti di Amazon Route 53, tra cui:

1. Le migliori pratiche DNS:
   - Comprendi i compromessi tra i valori TTL (time to live) e la reattività rispetto all'affidabilità.
   - Se possibile, utilizza i record alias anziché i record CNAME per migliorare le prestazioni e risparmiare sui costi.
   - Configura le politiche di routing predefinite per garantire che tutti i client ricevano una risposta.
   - Sfrutta il routing basato sulla latenza per ridurre al minimo la latenza delle applicazioni e il routing di geolocalizzazione/geoprossimità per stabilità e prevedibilità.
   - Verifica la propagazione delle modifiche utilizzando `GetChange` l'API per flussi di lavoro automatizzati.
   - Delega i sottodomini dalla zona principale per un routing coerente.
   - Evita risposte singole di grandi dimensioni utilizzando il routing delle risposte multivalore.
2. Le migliori pratiche di Resolver:
   - Previeni i loop di routing evitando di associare lo stesso VPC sia a una regola Resolver che al relativo endpoint in ingresso.
   - Implementa le regole dei gruppi di sicurezza per ridurre il sovraccarico di tracciamento delle connessioni e massimizzare la velocità di trasmissione delle query.
   - Configura gli endpoint in entrata con indirizzi IP in più zone di disponibilità per la ridondanza.
   - Fai attenzione ai potenziali attacchi DNS zone walking e contatta l' AWS assistenza se i tuoi endpoint subiscono un throttling.
3. Le migliori pratiche per i controlli sanitari:
   - Segui i consigli per ottimizzare i controlli di integrità di Amazon Route 53 per garantire un monitoraggio affidabile delle tue risorse

Aderendo a queste best practice, puoi ottimizzare le prestazioni, l'affidabilità e la sicurezza della tua infrastruttura DNS, garantendo un instradamento efficiente ed efficace del traffico verso le tue applicazioni e i tuoi servizi

Argomenti

- Le best practice per il Resolver
- Best practice per i controlli dell'integrità di Amazon Route 53

Le best practice per il DNS Amazon Route 53

Segui queste best practice per avere risultati ottimali utilizzando il DNS Amazon Route 53.

Utilizza le funzioni del piano dati per il failover DNS e il ripristino delle app

I piani dati per Route 53, compresi i controlli dello stato, e il controllo del routing di Amazon Application Recovery Controller (ARC) sono distribuiti a livello globale e sono progettati per garantire disponibilità e funzionalità al 100%, anche in caso di eventi gravi. Si integrano tra loro e non dipendono dalla funzionalità del piano di controllo. Pur essendo i piani di controllo per questi servizi, comprese le console, generalmente molto affidabili, sono progettati in modo più centralizzato e danno priorità alla durata e alla coerenza anziché all'elevata disponibilità. Per scenari come il failover durante il disaster recovery, ti consigliamo di utilizzare funzionalità come i controlli dello stato di Route 53 e il controllo del routing ARC che si basano sulla funzionalità del piano dati per aggiornare il DNS. Per ulteriori informazioni, consulta Nozioni sul piano di controllo e sul piano dati e Blog: Creating Disaster Recovery Mechanisms Using Amazon Route 53.

Scelta dei valori TTL per i registri DNS

Il TTL del DNS è il valore numerico (in secondi) utilizzato dai resolver DNS per decidere la durata di memorizzazione di un registro nella cache senza effettuare un'altra query su Route 53. Tutti i record DNS devono specificare un TTL. L'intervallo suggerito per i valori TTL è compreso tra 60 e 172.800 secondi.

La scelta di un TTL è un compromesso tra latenza, affidabilità e reattività al cambiamento. Se un record è più breve TTLs , i resolver DNS notano gli aggiornamenti del record più rapidamente in quanto devono eseguire query più frequentemente. Ciò aumenterà il volume (e il costo) della query. Man mano che il TTL si allunga, i resolver DNS rispondono alle query dalla cache più spesso, il che in genere è più veloce, più economico e, in alcune situazioni, più affidabile, perché evita le query su Internet. Non esiste un valore corretto, ma vale la pena riflettere su quanto sono importanti per i tuoi fini la reattività o l'affidabilità.

Aspetti da considerare durante l'impostazione dei valori TTL:

- Imposta il record DNS TTLs per il periodo di tempo che puoi permetterti di aspettare che una modifica abbia effetto. Ciò vale specialmente per le deleghe (set di registri NS) o altri registri

che raramente cambiano, ad esempio i registri MX. Per questi record, si consiglia un periodo più lungo TTLs . I valori comunemente usati sono compresi tra un'ora (3600 secondi) e un giorno (86.400 secondi).

- Per i record che devono essere modificati nell'ambito di un meccanismo di failover rapido (in particolare i record sottoposti a verifica dello stato di integrità), è consigliabile utilizzare un valore inferiore TTLs. Per questo scenario, è comune impostare un TTL di 60 o 120 secondi.
- Quando si desidera apportare modifiche alle voci DNS critiche, si consiglia di abbreviare temporaneamente le. TTLs Quindi puoi apportare le modifiche, osservare e ripristinare allo stato precedente se necessario. Dopo aver finalizzato le modifiche e se funzionano come previsto, puoi aumentare il TTL.

Per ulteriori informazioni, consulta TTL (secondi).

Registri CNAME

I registri CNAME del DNS sono un modo per passare da un nome dominio a un altro. Se un resolver DNS risolve domain-1.example.com e trova un CNAME che punta a domain-2.example.com, il resolver DNS deve procedere alla risoluzione domain-2.example.com prima che possa rispondere. Questi registri sono utili in molte situazioni, ad esempio per garantire la coerenza quando un sito Web ha più di un nome dominio.

Tuttavia, i resolver DNS devono effettuare più query a cui rispondere CNAMEs, il che aumenta la latenza e i costi. Ove possibile, un'alternativa più veloce ed economica consiste nell'utilizzare un registro alias di Route 53. I record di alias consentono a Route 53 di rispondere con una risposta diretta per AWS le risorse (ad esempio, un sistema di bilanciamento del carico) e per altri domini all'interno della stessa zona ospitata.

Per ulteriori informazioni, consulta Instradamento del traffico Internet verso le tue risorse AWS.

Routing DNS avanzato

- Quando uutilizzi il routing basato sulla geolocalizzazione, sulla geoprossimità o sulla latenza, imposta sempre un valore di default, a meno che non desideri che alcuni client ricevano nessuna risposta.
- Per minimizzare la latenza delle applicazioni, utilizza il routing basato sulla latenza. Questo tipo di dati di routing può cambiare frequentemente.
- Per assicurare la stabilità e la prevedibilità del routing, utilizza il routing basato sulla geolocalizzazione o sulla geoprossimità.

Per ulteriori informazioni, consulta Routing di geolocalizzazione, Routing di geoprossimità e Routing basato sulla latenza.

Propagazione della modifica DNS

Quando crei o aggiorni un record o una zona ospitata utilizzando la console o l'API Route 53, occorre del tempo prima che la modifica venga riflessa su Internet. Il processo si chiama propagazione delle modifiche. Sebbene di solito la propagazione richieda globalmente meno di un minuto, a volte può capitare che una modifica abbia un ritardo, ad esempio per problemi di sincronizzazione in una posizione o, in rari casi, per problemi interni al piano di controllo centrale. Se state creando flussi di lavoro di provisioning automatizzato ed è importante attendere il completamento della propagazione delle modifiche prima di procedere con la fase successiva del flusso di lavoro, utilizzate l'GetChangeAPI per verificare che le modifiche al DNS siano entrate in vigore (). `Status =INSYNC`

Delega DNS

Quando si delegano più livelli di sottodomini nel DNS, è importante che la delega venga effettuata sempre dalla zona madre. Ad esempio, se stai delegando www.dept.example.com, dovresti farlo dal dept.example.com zona, non dal example.com zona. Le deleghe da una zona nonna a una zona figlia potrebbero non funzionare o solo a tratti. Per ulteriori informazioni, consulta Routing del traffico per sottodomini.

Dimensioni della risposta del DNS

Evita di creare singole risposte di grandi dimensioni. Se le risposte eccedono i 512 byte, molti resolver DNS devono ripetere il tentativo su TCP anziché su UDP, il che può ridurre l'affidabilità e portare a un rallentamento delle risposte. Ti suggeriamo di utilizzare routing di risposte multivalore che scelgono 8 indirizzi IP integri e casuali per mantenere le risposte entro il limite di 512 byte.

Per ulteriori informazioni, consulta Routing di risposta multivalore e Test server delle dimensioni della risposta del DNS.

Le best practice per il Resolver

Questa sezione fornisce le best practice per ottimizzare Amazon Route 53 Resolver, trattando i seguenti argomenti:

1. Evitare configurazioni di loop con Resolver Endpoints:

- Previeni i loop di routing assicurandoti che lo stesso VPC non sia associato sia a una regola Resolver che al relativo endpoint in ingresso.
- Utilizzalo per condividere tra account mantenendo le configurazioni AWS RAM di routing corrette VPCs .

Per ulteriori informazioni, consulta Evitare configurazioni loop con endpoint di Resolver

2. Scalabilità degli endpoint Resolver:
   - Implementa regole di gruppo di sicurezza che consentano il traffico in base allo stato della connessione per ridurre il sovraccarico di tracciamento della connessione
   - Segui le regole consigliate sui gruppi di sicurezza per gli endpoint Resolver in entrata e in uscita per massimizzare la velocità di trasmissione delle query.
   - Monitora le combinazioni uniche di indirizzi IP e porte che generano traffico DNS per evitare limiti di capacità.

   Per ulteriori informazioni, consulta Dimensionamento dell'endpoint di Resolver
3. Alta disponibilità per gli endpoint Resolver:
   - Crea endpoint in entrata con indirizzi IP in almeno due zone di disponibilità per la ridondanza.
   - Fornisci interfacce di rete aggiuntive per garantire la disponibilità durante la manutenzione o i picchi di traffico

   Per ulteriori informazioni, consulta Alta disponibilità di endpoint di Resolver
4. Prevenzione degli attacchi DNS Zone Walking:
   - Fai attenzione ai potenziali attacchi DNS zone walking, in cui gli aggressori tentano di recuperare tutti i contenuti dalle zone DNS con firma DNSSEC.
   - Se i tuoi endpoint subiscono un rallentamento dovuto alla sospetta camminata in zona, contatta il Supporto AWS per ricevere assistenza.

   Per ulteriori informazioni, consulta Zona DNS

Seguendo queste best practice, è possibile ottimizzare le prestazioni, la scalabilità e la sicurezza delle implementazioni di Route 53 Resolver, garantendo una risoluzione DNS affidabile ed efficiente per le applicazioni e le risorse.

Evitare configurazioni loop con endpoint di Resolver

Non associare lo stesso VPC a una regola del Resolver e al relativo endpoint in entrata (sia che si tratti di una destinazione diretta dell'endpoint o tramite un server DNS on-premise). Quando l'endpoint in uscita in una regola Resolver punta a un endpoint in ingresso che condivide un VPC con la regola, può causare un ciclo in cui la query viene continuamente passata tra gli endpoint in entrata e in uscita.

La regola di inoltro può ancora essere associata ad altre regole condivise con altri account VPCs utilizzando (). AWS Resource Access Manager AWS RAM Le zone ospitate private associate all'hub o a un VPC centrale verranno comunque risolte dalle query agli endpoint in ingresso perché una regola del resolver di inoltro non modifica questa risoluzione.

Dimensionamento dell'endpoint di Resolver

I gruppi di sicurezza dell'endpoint di Resolver utilizzano il monitoraggio delle connessioni per raccogliere informazioni sul traffico da e verso gli endpoint. Ogni interfaccia di endpoint dispone di un numero massimo di connessioni che possono essere monitorate e un volume elevato di query DNS può superare le connessioni e causare limitazione e perdita di query. Per ridurre il numero di connessioni tracciate, implementare regole del gruppo di sicurezza che consentono il traffico in base allo stato di connessione del traffico. Per ulteriori informazioni, consulta Gruppi di sicurezza e tracciamento delle connessioni nella Amazon EC2 User Guide.

Le connessioni effettuate tramite applicazioni come Network Load Balancer e AWS Lambda (per un elenco completo vedi Connessioni tracciate automaticamente) vengono tracciate automaticamente, anche se la configurazione del gruppo di sicurezza non richiede altrimenti il tracciamento.

Se il tracciamento delle connessioni viene applicato utilizzando regole restrittive dei gruppi di sicurezza o le query vengono instradate tramite Network Load Balancer, il numero massimo complessivo di query al secondo per indirizzo IP per un endpoint può essere pari a 1500.

Raccomandazioni sulle regole del gruppo di sicurezza in ingresso e in uscita per l'endpoint Resolver in entrata

Regole di ingresso		
Tipo di protocollo	Numero della porta	IP di origine
TCP	53	0.0.0.0/0

UDP	53	0.0.0.0/0

Regole di uscita

Tipo di protocollo	Numero della porta	IP di destinazione
TCP	Tutti	0.0.0.0/0
UDP	Tutti	0.0.0.0/0

Raccomandazioni sulle regole del gruppo di sicurezza in ingresso e in uscita per l'endpoint Resolver in uscita

Regole di ingresso

Tipo di protocollo	Numero della porta	IP di origine
TCP	Tutti	0.0.0.0/0
UDP	Tutti	0.0.0.0/0

Regole di uscita

Tipo di protocollo	Numero della porta	IP di destinazione
TCP	Tutti	0.0.0.0/0
UDP	Tutti	0.0.0.0/0

Endpoint di Resolver in entrata

Per i client che utilizzano un endpoint di Resolver in ingresso, la capacità dell'interfaccia di rete elastica sarà influenzata se si dispone di oltre 40.000 combinazioni di indirizzi IP e porte univoche che generano il traffico DNS.

Alta disponibilità di endpoint di Resolver

Quando crei gli endpoint in ingresso del Resolver Route 53, il Route 53 richiede la creazione di almeno due indirizzi IP ai quali i resolver DNS della rete inoltreranno le query. Devi inoltre specificare gli indirizzi IP in almeno due zone di disponibilità per assicurare la ridondanza.

Se necessiti che siano sempre disponibili più endpoint dell'interfaccia di rete elastica, ti suggeriamo di creare almeno un'interfaccia di rete in più del necessario, così da disporre di capacità aggiuntiva per gestire eventuali picchi di traffico. L'interfaccia di rete aggiuntiva garantisce inoltre la disponibilità durante le operazioni di servizio, come la manutenzione o gli aggiornamenti.

Per ulteriori informazioni, consulta questo articolo dettagliato del blog: Come ottenere un'elevata disponibilità DNS con gli endpoint Route 53 Resolver e. Valori specificati durante la creazione o la modifica di endpoint in entrata

Zona DNS

Un attacco di zona DNS prova a ottenere tutto il contenuto dalle zone DNS firmate da DNSSEC. Se il team di Route 53 Resolver rileva un modello di traffico che corrisponde a quelli generati quando le zone DNS vengono spostate sull'endpoint, il team del servizio limiterà il traffico sull'endpoint. Di conseguenza, potresti osservare un'alta percentuale di query DNS che scadono.

Se osservi una capacità ridotta sui tuoi endpoint e ritieni che l'endpoint sia stato limitato erroneamente, vai su home#/ per creare una richiesta di supporto. https://console.aws.amazon.com/support/

Best practice per i controlli dell'integrità di Amazon Route 53

Una configurazione efficace per il controllo dello stato di salute è essenziale per mantenere un'infrastruttura ad alta disponibilità e resilienza. Ecco alcune best practice da considerare durante la configurazione e la gestione dei controlli sanitari di Amazon Route 53:

1. Utilizza indirizzi IP elastici per gli endpoint di controllo dello stato:
   - Utilizza indirizzi IP elastici per i tuoi endpoint di controllo sanitario per garantire un monitoraggio coerente.
   - Se non utilizzi più un' EC2 istanza Amazon, ricordati di eliminare tutti i controlli sanitari associati per evitare potenziali rischi per la sicurezza o compromissione dei dati.

Per ulteriori informazioni, consultaValori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità.

2. Configura gli intervalli appropriati per i controlli sanitari:
   - Imposta gli intervalli di controllo dello stato in base ai requisiti dell'applicazione e alla criticità delle risorse monitorate.
   - Intervalli più brevi garantiscono un rilevamento più rapido dei guasti, ma possono aumentare i costi di Route 53 e il carico di risorse.
   - Intervalli più lunghi riducono i costi e il carico di risorse, ma possono ritardare il rilevamento degli errori.

   Per ulteriori informazioni, vedereConfigurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint)).
3. Implementa le notifiche di allarme:
   - Configura Amazon CloudWatchalarms per ricevere notifiche quando i controlli sanitari falliscono o si ripristinano.
   - Imposta le soglie di allarme appropriate in base ai requisiti della tua applicazione e al comportamento previsto delle tue risorse.
   - Integra le notifiche con i tuoi processi di monitoraggio e risposta agli incidenti.

   Per ulteriori informazioni, consultaMonitoraggio dei controlli sanitari tramite CloudWatch.
4. Utilizza strategicamente le regioni per il controllo dello stato di salute:
   - Scegli le regioni per il controllo dello stato di salute in base alla distribuzione geografica degli utenti e delle risorse.
   - Valuta la possibilità di utilizzare più aree di controllo dello stato di salute per le risorse essenziali, al fine di migliorare l'affidabilità e ridurre l'impatto delle interruzioni regionali.
5. Monitora i registri e le metriche dei controlli sanitari:
   - Esamina regolarmente i registri e le CloudWatch metriche dei controlli dello stato di Route 53 per identificare potenziali problemi o rallentamenti delle prestazioni
   - Analizza i motivi del fallimento dei controlli sanitari e intraprendi le azioni appropriate per risolvere i problemi sottostanti.
6. Implementa strategie di failover e failback:
   - Sfrutta le policy di routing di failover di Route 53 per indirizzare automaticamente il traffico verso risorse integre in caso di guasti.

- Pianifica e testa i processi di failover e failback per garantire una transizione senza interruzioni durante le interruzioni e il ripristino.

Per ulteriori informazioni, vedere. Configurazione di un failover DNS

7. Rivedi e aggiorna regolarmente gli Health Checks:
   - Aggiorna gli endpoint, gli intervalli e le soglie di allarme dei controlli di integrità secondo necessità per mantenere il monitoraggio e le prestazioni ottimali.

Seguendo queste best practice, puoi sfruttare efficacemente i controlli dello stato di Amazon Route 53 per monitorare lo stato e la disponibilità delle nostre risorse, garantendo un'infrastruttura affidabile e ad alte prestazioni per le tue applicazioni e i tuoi servizi.

Quote

Le richieste API e le entità di Amazon Route 53 sono soggette alle seguenti quote (precedentemente denominate “limiti”).

Argomenti

Utilizzo di Service Quotas per visualizzare e gestire le quote

Puoi utilizzare il servizio Service Quotas per visualizzare le quote e richiederne un aumento per numerosi servizi AWS . Per maggiori informazioni, consulta Guida per l'utente di Service Quotas. Al momento puoi utilizzare le Service Quotas per visualizzare e gestire i domini e le quote di Route 53 e Route 53 Resolver.

> **Note**
>
> Per visualizzare le quote e richiedere quote più elevate per Route 53, è necessario modificare la regione in Stati Uniti orientali (Virginia settentrionale). Per visualizzare le quote e richiederne un aumento per Resolver, modifica la regione applicabile.

Quote relative alle entità

Le entità di Amazon Route 53 sono soggette alle quote descritte di seguito.

Per informazioni su come ottenere le quote correnti (precedentemente denominate “limiti”), consulta le seguenti operazioni di Route 53:

- GetAccountLimit— Ottiene quote sui controlli sanitari, sulle zone ospitate, sui set di deleghe riutilizzabili, sulle politiche di flusso del traffico e sui record delle politiche di flusso del traffico
- GetHostedZoneLimit— Ottiene quote sui record in una zona ospitata e su Amazon VPCs che è possibile associare a una zona ospitata privata

- GetReusableDelegationSetLimit— Ottiene la quota del numero di zone ospitate che è possibile associare a un set di deleghe riutilizzabile

Argomenti

Quote relative ai domini

Entità	Quota
Domini	20* per account AWS Richiedi una quota più elevata.

*Il limite è 20 per i nuovi clienti a partire da marzo 2021.

Se hai un account esistente e il tuo limite di default è 50, rimarrà a 50.

Quote relative alle zone ospitate

Entità	Quota
Zona ospitata	Quota iniziale di 500 per AWS account, ma puoi richieder e una quota superiore se necessario.

Entità	Quota
	Richiedi una quota più elevata.
Hosted zone che possono usare lo stesso set di deleghe riutilizzabili	100 Richiedi una quota più elevata.
Amazon VPCs che puoi associare a una zona ospitata privata per zona ospitata	300 Se desideri più di 300 associazioni, ti consigliamo di utilizzare i profili Route 53. Per ulteriori informazioni, consulta Cosa sono i profili Amazon Route 53?.
Zone ospitate private che è possibile associare a un VPC	Nessuna quota *
Autorizzazioni che puoi creare in modo da VPCs poter associare quelle create da un account a una zona ospitata creata da un altro account	1000
Il numero di chiavi di firma delle chiavi (KSK) che è possibile creare per zona ospitata	2

* Puoi associare un VPC a una o tutte le zone private ospitate che controlli tramite i tuoi AWS account. Ad esempio, supponiamo di avere tre AWS account e che tutti e tre abbiano la quota predefinita di 500 zone ospitate. Se si creano 500 zone ospitate private per tutti e tre gli account, è possibile associare un VPC a tutte le 1.500 zone ospitate private.

Quote relative ai record

Entità	Quota
Registri	10.000 per zona ospitata Richiedi una quota più elevata. Per una quota superiore a 10.000 registri in una zona ospitata si applica un costo aggiuntivo. Per ulteriori informazioni, consulta la sezione Prezzi di Amazon Route 53.
Record in un set di record	400 per set di record
Record di geolocalizzazione, risposta multivalore, latenza, ponderati e basati su IP	100 record con lo stesso nome e tipo
Record di geoprossimità	30 record con lo stesso nome e tipo
Raccolte CIDR	5 per. Account AWS Richiedi una quota più elevata.
Blocchi CIDR	1000 per raccolta CIDR. Richiedi una quota più elevata.

Quote relative a Route 53 Resolver

In questa sezione sono incluse tutte le quote Route 53 Resolver

Quote relative a Route 53 Resolver

Utilizza la procedura seguente per aumentare le quote per Route 53 Resolver.

Come aumentare le quote di Resolver

1. Apri la console Service Quotas all'indirizzo https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas.
2. Passa alla regione in cui desideri aumentare il limite.
3. Seleziona il nome della quota di Route 53 Resolver che desideri aumentare.
4. Seleziona Richiedi aumento di quota, specifica il valore della quota, quindi seleziona Richiesta.

Quote relative agli endpoint Route 53 Resolver

Entità	Quota
Endpoint per regione AWS	4 per account AWS Richiedi una quota più elevata.
indirizzi IP per endpoint	6 Richiedi una quota più elevata.
Indirizzi IP per regola	6
Regole per AWS regione	1000 per AWS account Richiedi una quota più elevata.
Associazioni tra regole e VPCs per AWS regione	2000 per AWS account Richiedi una quota più elevata.
Query UDP al secondo per indirizzo IP in un endpoint	10.000*

* Ogni indirizzo IP in un endpoint può elaborare fino a 10.000 query DNS UDP al secondo (QPS). Il numero di QPS DNS varia in base al tipo di query, alle dimensioni della risposta, all'integrità dei server dei nomi di destinazione, ai tempi di risposta delle query,alla latenza di andata e ritorno e al protocollo in uso. Ad esempio, le query a un server dei nomi di destinazione che è lento a rispondere possono ridurre significativamente la capacità dell'interfaccia di rete. Inoltre, per garantire la disponibilità elevata, Route 53 Resolver genera query in uscita ridondanti per ogni richiesta DNS che riceve. Di conseguenza, il QPS per ogni interfaccia di rete in uscita non corrisponderà al QPS inviato a Route 53 Resolver. Utilizza le CloudWatch metriche per misurare quante query vengono inviate a ciascuna interfaccia di rete. Per ulteriori informazioni, consulta Parametri per gli indirizzi IP di Resolver. Se la frequenza massima di query supera il 50% della capacità per qualsiasi interfaccia di rete nell'endpoint, puoi aggiungere altre interfacce di rete per aumentare la capacità dell'endpoint.

Le connessioni effettuate tramite applicazioni come Network Load Balancer e AWS Lambda (per un elenco completo vedi Connessioni tracciate automaticamente) vengono tracciate automaticamente, anche se la configurazione del gruppo di sicurezza non richiede altrimenti il tracciamento.

Se il tracciamento delle connessioni viene applicato utilizzando regole restrittive dei gruppi di sicurezza o le query vengono instradate tramite Network Load Balancer, il numero massimo complessivo di query al secondo per indirizzo IP per un endpoint in ingresso può essere pari a 1500.

Quote dei log di query di Route 53 Resolver

Entità	Quota
Configurazioni dei log di query per regione AWS	20
Associazioni VPC di configurazione dei log di query per regione* AWS	100
Associazioni VPC di configurazione dei log di query per account per regione AWS (condivise tramite RAM) per l'account con cui è stata condivisa la configurazione.	100

* Questo è un limite non modificabile. Non è possibile creare un'altra configurazione del registro delle query nella stessa configurazione Regione AWS e VPCs associarvi altre 100.

Quote su DNS Firewall per Route 53 Resolver

Entità	Quota
Numero di gruppi di regole associati a un VPC per un singolo account per regione AWS	5
Numero di domini DNS Firewall in un singolo file Amazon S3 per un singolo account per regione AWS	250.000 Richiedi una quota più elevata.
Numero di gruppi di regole DNS Firewall per un singolo account per regione AWS	1.000 Richiedi una quota più elevata.
Numero di regole all'interno di un gruppo di regole per un singolo account per regione AWS	100 Richiedi una quota più elevata.
Numero di elenchi di domini per un singolo account per AWS regione	1000 Richiedi una quota più elevata.
Il numero massimo di domini che è possibile specificare in tutti gli elenchi di domini per un singolo account per regione AWS	100.000 Richiedi una quota più elevata.

Quote su Resolver su Outpost

Entità	Quota
Limite di istanze di Resolver su Outpost	6 (con un minimo di 4 richieste)

Resolver sui tipi di istanza Outpost e il numero di query DNS al secondo che ogni tipo di istanza può supportare:

Tipo di istanza	Query al secondo
c5.large	Fino a 7.000
c5.xlarge	Fino a 12.000
c5.2xlarge	Fino a 24.000
c5.4xlarge	Fino a 56.000
c5d.large	Fino a 7.000
c5d.xlarge	Fino a 12.000
c5d.2xlarge	Fino a 24.000
c5d.4xlarge	Fino a 56.000
m5.large	Fino a 7.000
m5.xlarge	Fino a 12.000

Tipo di istanza	Query al secondo
m5.2xlarge	Fino a 24.000
m5.4xlarge	Fino a 56.000
m5d.large	Fino a 7.000
m5d.xlarge	Fino a 12.000
m5d.2xlarge	Fino a 24.000
m5d.4xlarge	Fino a 56.000
r5.large	Fino a 7.000
r5.xlarge	Fino a 12.000
r5.2xlarge	Fino a 24.000
r5.4xlarge	Fino a 56.000
r5d.large	Fino a 7.000
r5d.xlarge	Fino a 12.000
r5d.2xlarge	Fino a 24.000
r5d.4xlarge	Fino a 56.000

I tipi di istanza degli endpoint Resolver on Outpost e il numero di query DNS al secondo che ogni tipo di istanza può supportare:

Tipo di istanza	Query al secondo
c5.large	Fino a 5.000
c5.xlarge	Fino a 10.000
c5.2xlarge	Fino a 18.000
c5.4xlarge	Fino a 30.000
c5d.large	Fino a 5.000
c5d.xlarge	Fino a 10.000
c5d.2xlarge	Fino a 18.000
c5d.4xlarge	Fino a 30.000
m5.large	Fino a 5.000
m5.xlarge	Fino a 10.000
m5.2xlarge	Fino a 18.000
m5.4xlarge	Fino a 30.000
m5d.large	Fino a 5.000
m5d.xlarge	Fino a 10.000

Tipo di istanza	Query al secondo
m5d.2xlarge	Fino a 18.000
m5d.4xlarge	Fino a 30.000
r5.large	Fino a 5.000
r5.xlarge	Fino a 10.000
r5.2xlarge	Fino a 18.000
r5.4xlarge	Fino a 30.000
r5d.large	Fino a 5.000
r5d.xlarge	Fino a 10.000
r5d.2xlarge	Fino a 18.000
r5d.4xlarge	Fino a 30.000

Quote relative ai controlli dell'integrità

Entità	Quota
Controlli dell'integrità	200 controlli sanitari attivi per account AWS Richiedi una quota più elevata.
	255

Entità	Quota
Controlli dello stato figlio che un controllo dell'integrità calcolato può monitorare	
Lunghezza totale massima delle intestazioni nella risposta a una richiesta di controllo dell'integrità	16.384 byte (16K)

Quote relative alle configurazioni dei log di query

Entità	Quota
Configurazioni dei log di query	1 per zona ospitata

Quote relative alle policy sul flusso di traffico e ai record delle policy

Entità	Quota
Policy sul traffico Per ulteriori informazioni sul flusso di traffico di Route 53, consulta Utilizzo di Traffic Flow per instradare il traffico DNS.	50 per AWS account Richiedi una quota più elevata.
Versioni di policy di traffico	1.000 per policy di traffico
Record relativi alle politiche sul traffico (denominati «istanze di policy» nell'API Route 53, AWS SDKs AWS Command Line	5 per account AWS Richiedi una quota più elevata.

Entità	Quota
Interface, e AWS Tools for Windows PowerShell)	

Quote sui set di deleghe riutilizzabili

Entità	Quota
Set di deleghe riutilizzabili	100 per AWS account Richiedi una quota più elevata.

Quote sui profili della Route 53

Entità	Quota
Numero di profili Route 53 per Account AWS regione	5 Richiedi una quota più elevata.
Numero di VPCs questi può essere associato a un profilo	1000 Richiedi una quota più elevata.
Numero di gruppi di regole DNS Firewall per profilo	5
Numero di regole Resolver per profilo	1000 Richiedi una quota più elevata.
Numero di zone private ospitate per profilo	1.000 Richiedi una quota più elevata.

Valori massimi relativi alle richieste API

Le richieste API di Amazon Route 53 sono soggette ai valori massimi descritti di seguito.

Argomenti

Numero di elementi e caratteri nelle richieste **`ChangeResourceRecordSets`**

Elementi **`ResourceRecord`**

Una richiesta non può contenere più di 1.000 elementi `ResourceRecord` (compresi i registri alias). Quando il valore dell'elemento `Action` è `UPSERT`, ciascun elemento `ResourceRecord` viene calcolato due volte.

Numero massimo di caratteri

La somma del numero di caratteri (spazi inclusi) in tutti gli elementi `Value` in una richiesta non può superare i 32.000 caratteri. Quando il valore dell'elemento `Action` è `UPSERT`, ciascun carattere in un elemento `Value` viene calcolato due volte.

Frequenza delle richieste API di Amazon Route 53

Tutte le richieste API di Amazon Route 53

Per Amazon Route 53 APIs cinque richieste al secondo per AWS account. Se invii più di cinque richieste al secondo, Amazon Route 53 restituisce un errore HTTP 400 (`Bad request`). L'intestazione di risposta include anche un elemento `Code` con un valore `Throttling` e un elemento `Message` con un valore di `Rate exceeded`.

> **Note**
>
> Se la tua applicazione supera questo limite, ti suggeriamo di implementare il backoff esponenziale per i tentativi. Per ulteriori informazioni, consulta Ripetizione dei tentativi in

caso di errore e backoff esponenziale in AWS nella Riferimenti generali di Amazon Web Services.

Richieste **`ChangeResourceRecordSets`**

Se Route 53 non è in grado di elaborare una richiesta prima che arrivi la richiesta successiva, respingerà le richieste successive per la stessa zona ospitata e restituirà un errore HTTP 400 (`Bad request`). L'intestazione di risposta include anche un elemento `Code` con un valore `PriorRequestNotComplete` e un elemento `Message` con un valore di `The request was rejected because Route 53 was still processing a prior request.`

Richieste **`CreateHealthCheck`**

Puoi inviare una `CreateHealthCheck` richiesta ogni 2 secondi per Account AWS.

Frequenza delle richieste API di Resolver Route 53

Tutte le richieste

Cinque richieste al secondo per AWS account per regione. Se invii più di cinque richieste al secondo in una regione, Resolver restituisce un errore HTTP 400 (`Bad request`). L'intestazione di risposta include anche un elemento `Code` con un valore `Throttling` e un elemento `Message` con un valore di `Rate exceeded`.

> **Note**
>
> Se la tua applicazione supera questo limite, ti suggeriamo di implementare il backoff esponenziale per i tentativi. Per ulteriori informazioni, consulta Ripetizione dei tentativi in caso di errore e backoff esponenziale in AWS nella Riferimenti generali di Amazon Web Services.

Informazioni correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

Argomenti

- AWS risorse
- Librerie e strumenti di terze parti
- Interfacce utente grafiche

AWS risorse

Amazon Web Services rende disponibili numerose guide, forum e altre risorse utili.

- Documentazione di riferimento dell'API di Amazon Route 53: una guida di riferimento che include posizione dello schema, descrizioni di operazioni, parametri e tipi di dati API e un elenco di errori generati dal servizio.
- AWS::Route53::RecordSetDigita la Guida per AWS CloudFormation l'utente: una proprietà con cui usare Amazon Route 53 AWS CloudFormation per creare nomi DNS personalizzati per i tuoi AWS CloudFormation stack.
- Forum di discussione: forum basato su una community per sviluppatori dedicato alla discussione di domande tecniche correlate a Route 53.
- AWS Support Center: questo sito raccoglie informazioni sui casi di supporto recenti e sui risultati dei controlli di AWS Trusted Advisor e dello stato di salute, oltre a fornire collegamenti a forum di discussione, informazioni tecniche FAQs, il pannello di controllo dello stato del servizio e informazioni sui piani di AWS supporto.
- AWS Informazioni sull'assistenza Premium: la pagina Web principale per informazioni su AWS Premium Support one-on-one, un canale di supporto a risposta rapida che consente di creare ed eseguire applicazioni su AWS Infrastructure Services.
- Contattaci: collegamenti per domande su fatturazione o account. Per quesiti tecnici, utilizzare i forum di discussione o i collegamenti di supporto elencati sopra.
- Informazioni sul prodotto: la pagina Web principale che include informazioni su Route 53, incluse le caratteristiche, le informazioni sui prezzi e altro ancora.

- Corsi e workshop: collegamenti a corsi specializzati e basati su ruoli, oltre a laboratori di autoapprendimento per affinare le competenze e acquisire esperienza pratica. AWS
- AWS Developer Center: esplora i tutorial, scarica strumenti e scopri gli eventi per sviluppatori. AWS
- AWS Strumenti per sviluppatori: collegamenti a strumenti di sviluppo SDKs, toolkit IDE e strumenti da riga di comando per lo sviluppo e la gestione di applicazioni. AWS
- Centro risorse introduttivo: scopri come configurare Account AWS, entrare a far parte della AWS community e lanciare la tua prima applicazione.
- Tutorial pratici: segui i tutorial per avviare la step-by-step tua prima applicazione su. AWS
- AWS Whitepaper: collegamenti a un elenco completo di AWS white paper tecnici, su argomenti quali architettura, sicurezza ed economia e redatti da Solutions Architects o altri esperti tecnici. AWS
- Supporto AWS Center: l'hub per la creazione e la gestione dei casi. Supporto AWS Include anche collegamenti ad altre risorse utili, come forum, informazioni tecniche FAQs, stato di salute del servizio e AWS Trusted Advisor.
- Supporto— La pagina web principale per informazioni su Supporto one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contatti - Un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS .
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito e altri argomenti.

Librerie e strumenti di terze parti

Oltre alle AWS risorse, puoi trovare una varietà di strumenti e librerie di terze parti compatibili con Amazon Route 53.

- AmazonRoute53 AppsScript (tramite webos-goodies)

  Gestione di fogli di calcolo Google di Amazon Route 53.

- AWS Componente per.NET (via) SprightlySoft

  SprightlySoft Componente.NET per Amazon Web Services con supporto per operazioni REST e Route 53.

- Download API Boto (tramite github)

Interfaccia Boto Python ad Amazon Web Services.

- cli53 (tramite github)

  Interfaccia a riga di comando per Route 53.

- Dasein Cloud API

  API basata su Java.

- R53.py (tramite github)

  Mantiene una versione canonica delle configurazioni DNS sotto il controllo del codice sorgente e calcola l'insieme minimo di modifiche necessarie per modificare una configurazione.

- route53d

  Front-end DNS per l'API Route 53 (consente il trasferimento di zona incrementale (IXFR)).

- Route53Manager (tramite github)

  Interfaccia basata sul Web.

- Ruby Fog (tramite github)

  La libreria di servizi cloud Ruby.

- WebService: :Amazon: :Route53 (tramite CPAN)

  Interfaccia Perl per l'API Amazon Route 53.

Interfacce utente grafiche

I seguenti strumenti di terze parti forniscono interfacce utente grafiche (GUIs) per lavorare con Amazon Route 53:

- R53 Fox
- Ylastic

Cronologia dei documenti

Le voci seguenti descrivono le modifiche importanti in ciascuna versione della documentazione di Route 53. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

Argomenti

Versioni 2025

14 gennaio 2025

Amazon Route 53 ora supporta i record di alias per gli endpoint di dominio personalizzati del OpenSearch Servizio. Per ulteriori informazioni, consulta Instradamento del traffico verso l'endpoint OpenSearch del dominio Amazon Service.

13 gennaio 2025

Aggiunti i risultati del firewall DNS di Route 53 Resolver al Security Hub. Per ulteriori informazioni, consulta Invio dei risultati dal firewall DNS di Route 53 Resolver al Security Hub.

Versioni 2024

15 novembre 2024

È stato aggiunto Route 53 Resolver DNS Firewall Advanced, un nuovo set di funzionalità su Route 53 Resolver DNS Firewall che consente di identificare e bloccare il traffico DNS associato a minacce DNS avanzate, come il tunneling DNS e le minacce basate su Domain Generation Algorithm (DGA). Per ulteriori informazioni, consulta Route 53 Resolver DNS Firewall avanzato.

29 ottobre 2024

È stato aggiunto il supporto per i tipi di record DNS HTTPS, SSHFP, SVCB e TLSA. Per ulteriori informazioni, consulta Tipi di record DNS supportati.

3 ottobre 2024

È stato aggiunto il supporto per Service Name Indication (SNI) per gli endpoint Resolver in uscita DoH. Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica delle regole.

3 settembre 2024

Ora puoi utilizzare le condizioni delle `route53:VPCs` politiche per concedere un accesso granulare alla gestione delle associazioni di zone ospitate a. VPCs Per ulteriori informazioni, consulta Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi.

27 agosto 2024

`AmazonRoute53ProfilesFullAccess`ha aggiunto autorizzazioni per `GetProfilePolicy` e. `PutProfilePolicy` Si tratta di operazioni IAM che richiedono solo l'autorizzazione. Se a un preside IAM non sono concesse queste autorizzazioni, si verificherà un errore durante il tentativo di condividere il profilo utilizzando il servizio. AWS RAM Per ulteriori informazioni, consulta AWS politica gestita: 53 AmazonRoute ProfilesFullAccess.

27 agosto 2024

`AmazonRoute53ProfilesReadOnlyAccess`ha aggiunto l'autorizzazione per`GetProfilePolicy`. Questa è un'azione IAM che richiede solo l'autorizzazione. Se a

un principale IAM non viene concessa questa autorizzazione, si verificherà un errore durante il tentativo di accedere alla politica del profilo utilizzando il servizio. AWS RAM Per ulteriori informazioni, consulta AWS politica gestita: 53 AmazonRoute ProfilesReadOnlyAccess.

5 agosto 2024

È stato aggiunto un ID di dichiarazione (Sid) per identificare in modo univoco la policy gestita. `AmazonRoute53ResolverFullAccess` Per ulteriori informazioni, consulta AWS politica gestita: 53 AmazonRoute ResolverFullAccess.

5 agosto 2024

È stato aggiunto un ID di dichiarazione (Sid) per identificare in modo univoco la policy gestita. `AmazonRoute53ResolverReadOnlyAccess` Per ulteriori informazioni, consulta AWS politica gestita: 53 AmazonRoute ResolverReadOnlyAccess.

18 luglio 2024

Ha aggiornato l'intera guida Route 53 con la nuova esperienza da console per i controlli sanitari. Per ulteriori informazioni, consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.

30 aprile 2024

Ora puoi decidere se una regola del firewall DNS ispezionerà (impostazione predefinita) o considererà attendibile la catena di reindirizzamento DNS. Per ulteriori informazioni, consulta Componenti e impostazioni di DNS Firewall per Route 53 Resolver e Impostazioni delle regole in DNS Firewall.

22 aprile 2024

Ora puoi utilizzare i profili Route 53 per condividere configurazioni DNS specifiche con molti VPCs e con account. AWS Per ulteriori informazioni, consulta Cosa sono i profili Amazon Route 53?.

22 aprile 2024

Sono state aggiunte le policy gestite `AmazonRoute53ProfilesReadOnlyAccess` e `AmazonRoute53ProfilesFullAccess` l'accesso completo e in sola lettura ai profili Amazon Route 53. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon Route 53.

5 febbraio 2024

Ora puoi usare Amazon EventBridge per avvisi in tempo reale con DNS Firewall. Per ulteriori informazioni, consulta Gestione degli eventi del firewall DNS di Route 53 Resolver utilizzando Amazon EventBridge.

9 gennaio 2024

Ora puoi utilizzare il tipo di query DNS come valore opzionale per la regola DNS Firewall per differenziare la risposta della regola per un tipo di query DNS specifico. Per ulteriori informazioni, consulta Componenti e impostazioni di DNS Firewall per Route 53 Resolver e Impostazioni delle regole in DNS Firewall.

9 gennaio 2024

È ora possibile utilizzare il record di creazione rapida o la procedura guidata di creazione di record per creare record di routing di geoprossimità. Per ulteriori informazioni, consulta Routing di geoprossimità, Valori specifici per i record di geoprossimità e Valori specifici per i record di alias di geoprossimità.

Rilasci 2023

20 dicembre 2023

Ora puoi utilizzare DNS su HTTPS con gli endpoint Route 53 Resolver. Per ulteriori informazioni, consulta Scelta dei protocolli per gli endpoint.

20 luglio 2023

Amazon Route 53 on Outposts è ora disponibile su AWS Outposts rack. Include un Resolver che memorizza nella cache tutte le query DNS provenienti da AWS Outposts. Puoi impostare anche una connettività ibrida tra un Outpost e un resolver DNS on-premise quando metti in produzione endpoint in entrata e in uscita. Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 on Outposts?.

19 luglio 2023

Ora, una volta abilitate, puoi usare le zone locali con l'instradamento di geoprossimità (solo per il flusso di traffico). Per ulteriori informazioni, consulta Routing di geoprossimità e Formato del documento della policy di traffico.

22 marzo 2023

Aggiornata l'intera guida Route 53 con l'esperienza della nuova console per i domini. Puoi anche utilizzare la nuova esperienza della console per trasferire un dominio da uno Account AWS all'altro Account AWS. Per ulteriori informazioni, consulta Registrazione di un nuovo dominio e Trasferimento dei domini.

10 marzo 2023

Ora puoi connetterti alle tue risorse utilizzando o utilizzando IPv4 IPv6 endpoint dual-stack con. Amazon Route 53 Resolver Per ulteriori informazioni, consulta Valori specificati durante la creazione o la modifica di endpoint in entrata e Valori specificati durante la creazione o la modifica degli endpoint in uscita.

Rilasci 2022

21 settembre 2022

Puoi utilizzare le condizioni delle policy per fornire agli utenti un accesso granulare all'aggiornamento dei set di record di risorse in Amazon Route 53. Per ulteriori informazioni, consulta Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi.

30 agosto 2022

Amazon Route 53 ora supporta i record di alias per AWS App Runner i servizi creati dopo il 1° agosto 2022. Per ulteriori informazioni, consulta Instradamento del traffico verso un servizio AWS App Runner.

1 giugno 2022

L'opzione di routing basata su IP è ora disponibile in Amazon Route 53. Per ulteriori informazioni, consulta Routing basato su IP.

16 marzo 2022

Le opzioni di routing basato sulla geolocalizzazione e sulla latenza sono ora supportate per le zone ospitate private in Amazon Route 53. Per ulteriori informazioni, consulta Considerazioni sull'utilizzo di una zona ospitata privata.

25 gennaio 2022

Il processo di modifica della proprietà di .com.au e .net.au TLDs è stato semplificato per includere la risposta a due e-mail (da parte dei vecchi e dei nuovi registranti) e non include la compilazione di moduli. Per ulteriori informazioni, consulta .com.au (Australia) e .net.au (Australia).

Rilasci 2021

26 ottobre 2021

Aggiunto il supporto per la disattivazione delle regole DNS inverse predefinite con Amazon Route 53. Ora è possibile disabilitare la creazione di queste regole e inoltrare invece le query per gli spazi dei nomi DNS inversi a server esterni, se lo si desidera. Per ulteriori informazioni, consulta Regole di inoltro per le query DNS inverse in Resolver.

1 settembre 2021

È stato aggiunto un nuovo argomento introduttivo che illustra la creazione di CloudFront distribuzioni Amazon per un sito Web statico. Per ulteriori informazioni, consulta Usa una CloudFront distribuzione Amazon per servire un sito Web statico.

14 luglio 2021

Ha iniziato a tracciare le politiche AWS gestite per Amazon Route 53. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon Route 53.

31 marzo 2021

Aggiunto DNS Firewall per Route 53 Resolver. Con DNS Firewall puoi fornire protezione per le richieste DNS in uscita provenienti da... VPCs Per ulteriori informazioni, consulta Utilizzo di DNS Firewall per filtrare il traffico DNS in uscita.

Rilasci 2020

17 dicembre 2020

Aggiunto il supporto per la firma DNSSEC per Route 53 Resolver. Per ulteriori informazioni, consulta Configurazione della firma DNSSEC in Amazon Route 53.

Aggiunto il supporto per la convalida DNSSEC per Route 53 Resolver. Per ulteriori informazioni, consulta Abilitazione della convalida DNSSEC in Amazon Route 53.

23 settembre 2020

Aggiornata l'intera guida Route 53 con l'uso della nuova console. Per ulteriori informazioni, consulta Che cos'è Amazon Route 53?.

1 settembre 2020

Aggiunto il supporto per i log delle query di Resolver. Per ulteriori informazioni, consulta Registrazione delle query di Resolver.

Versioni 2018

20 dicembre 2018

Puoi creare record di alias Route 53 che indirizzano il traffico verso API Gateway APIs o verso gli endpoint dell'interfaccia Amazon VPC. Per ulteriori informazioni, consulta Valore/instradamento traffico a.

28 novembre 2018

Route 53 Auto Naming (noto anche come Service Discovery) è ora un servizio separato,. AWS Cloud Map Per ulteriori informazioni, consulta la Guida per gli sviluppatori di AWS Cloud Map.

19 novembre 2018

Puoi utilizzare Route 53 Resolver per configurare la risoluzione DNS tra il VPC e la rete tramite Direct Connect o una connessione VPN. (Resolver è il nuovo nome del servizio DNS ricorsivo che viene fornito a tutti i clienti per impostazione predefinita in Amazon Virtual Private Cloud (Amazon VPC).) Questo consente di inoltrare query DNS dai resolver sulla rete a Route 53 Resolver. Resolver consente anche di inoltrare le query per nomi di dominio selezionati (example.com) e i nomi di sottodominio (api.example.com) da un VPC ai resolver sulla rete. Per ulteriori informazioni, consulta Che cos'è Amazon Route 53 Resolver?.

7 novembre 2018

Quando utilizzi Route 53 Traffic Flow e il routing di geoprossimità, puoi utilizzare una mappa interattiva per visualizzare la modalità di instradamento degli utenti finali agli endpoint in tutto il modo. Per ulteriori informazioni, consulta Visualizzazione di una mappa che mostra l'effetto delle impostazioni sulla geoprossimità.

18 ottobre 2018

Puoi utilizzare la console e l'API di Route 53 per disabilitare temporaneamente un controllo dell'integrità di Route 53. Questo offre un modo semplice per sospendere il monitoraggio di un endpoint, ad esempio un server Web, in modo da poterne eseguire la manutenzione senza attivare allarmi o generare log o messaggi di stato non necessari. Per ulteriori informazioni,

consulta "Disabilitato" in Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità. La funzionalità è disponibile per tutti e tre i tipi di controlli di integrità di Route 53: controlli di integrità che monitorano un endpoint, controlli di integrità che monitorano altri controlli di integrità e controlli di integrità che monitorano un CloudWatch allarme.

13 marzo 2018

Se stai utilizzando l'auto-denominazione, ora puoi usare uno strumento di controllo dell'integrità di terza parte per valutare lo stato delle tue risorse. È utile quando una risorsa non è disponibile su Internet, ad esempio perché l'istanza è un Amazon VPC. Per ulteriori informazioni, HealthCheckCustomConfigconsulta Amazon Route 53 API Reference.

9 marzo 2018

IAM comprende ora policy gestite per l'auto-denominazione. Per ulteriori informazioni, consulta AWS politiche gestite per Amazon Route 53.

6 febbraio 2018

Ora puoi configurare l'auto-denominazione per creare record alias che instradino il traffico a sistemi di bilanciamento del carico ELB o per creare record CNAME. Per ulteriori informazioni, consulta Attributi nella documentazione per l'RegisterInstanceAPI nell'Amazon Route 53 API Reference.

Versioni 2017

5 dicembre 2017

È ora possibile utilizzare l'API di denominazione automatica di Route 53 per effettuare il provisioning di istanze per i microservizi. La denominazione automatica ti consente di creare automaticamente i record DNS e, facoltativamente, i controlli dell'integrità in base a un modello da te definito. Per ulteriori informazioni, consulta Cos'è AWS Cloud Map? nella Guida per gli AWS Cloud Map sviluppatori.

16 novembre 2017

Ora è possibile ottenere a livello di codice sia le quote attuali delle risorse Route 53, ad esempio le zone ospitate e i controlli dell'integrità, sia il numero di ciascuna risorsa attualmente in uso. Per ulteriori informazioni GetAccountLimitGetHostedZoneLimit, consulta e GetReusableDelegationSetLimitconsulta Amazon Route 53 API Reference.

3 ottobre 2017

Route 53 è ora un servizio idoneo ai fini HIPAA. Per ulteriori informazioni, consulta Convalida della conformità per Amazon Route 53.

29 settembre 2017

Ora puoi controllare dal punto di vista programmatico se un dominio può essere trasferito a Route 53. Per ulteriori informazioni, CheckDomainTransferabilityconsulta Amazon Route 53 API Reference.

11 settembre 2017

Ora puoi creare record alias Route 53 per instradare il traffico Internet a bilanciatori del carico di rete di Elastic Load Balancing. Per ulteriori informazioni sui record alias, consulta Scelta tra record alias e non alias.

7 settembre 2017

Se usi Route 53 come il tuo servizio DNS pubblico autorevole, ora puoi registrare le query DNS ricevute da Route 53. Per ulteriori informazioni, consulta Registrazione delle query DNS pubbliche.

1 settembre 2017

Se usi il flusso di traffico di Route 53, puoi utilizzare il routing di geoprossimità che consente di instradare il traffico in base alla distanza fisica tra i tuoi utenti e le tue risorse. Puoi anche instradare più o meno traffico a ciascuna risorsa specificando un bias positivo o negativo. Per ulteriori informazioni, consulta Routing di geoprossimità.

21 agosto 2017

Puoi ora utilizzare Route 53 per creare record di autorizzazione della certification authority (CAA) che consentono di specificare le certification authority che sono in grado di emettere certificati per i tuoi domini e sottodomini. Per ulteriori informazioni, consulta Tipo di record CAA.

18 agosto 2017

Ora puoi trasferire grandi quantità di domini a Route 53 utilizzando la console Route 53. Per ulteriori informazioni, consulta Trasferimento della registrazione per un dominio ad Amazon Route 53.

4 agosto 2017

Quando registri un dominio, i registri di alcuni domini di primo livello (TLDs) richiedono la verifica di aver specificato un indirizzo e-mail valido per il contatto del registrante. Puoi ora inviare l'e-

mail di verifica e ricevere conferma che è stato possibile verificare l'indirizzo e-mail durante la procedura di registrazione del dominio. Per ulteriori informazioni, consulta Registrazione di un nuovo dominio.

21 giugno 2017

Se desideri instradare il traffico in modo casuale a più risorse, ad esempio server Web, puoi ora creare un record di risposta multivalore per ciascuna risorsa e, facoltativamente, associare un controllo dell'integrità di Route 53 a ogni record. Route 53 risponde alle query DNS con un massimo di otto record integri in risposta a ciascuna query DNS e offre diverse risposte a diversi resolver DNS. Per ulteriori informazioni, consulta Routing di risposta multivalore.

10 aprile 2017

Quando utilizzi la console Route 53 per trasferire la registrazione di un dominio a Route 53, ora puoi scegliere una delle seguenti opzioni per associare i server dei nomi per il servizio DNS per il dominio alla registrazione del dominio trasferito:

- Utilizza i server dei nomi per una zona ospitata Route 53 scelta
- Utilizza i server di nomi per l'attuale servizio DNS per il dominio
- Utilizza i server di nomi che specifichi

Route 53 associa automaticamente questi server dei nomi alla registrazione del dominio trasferito.

Versioni 2016

21 novembre 2016

Ora puoi creare controlli di integrità che utilizzano IPv6 indirizzi per verificare lo stato degli endpoint. Per ulteriori informazioni, consulta Creazione e aggiornamento di controlli dell'integrità.

15 novembre 2016

Ora puoi utilizzare una operazione API Route 53 per associare un Amazon VPC creato con un account con una zona ospitata privata creata con un altro account. Per ulteriori informazioni, consulta Associazione di un Amazon VPC e una zona ospitata privata creata con account diversi AWS.

30 agosto 2016

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Record Name Authority Pointer (NAPTR): ora puoi creare record NAPTR, un tipo di registro utilizzato dalle applicazioni DDDS (Dynamic Delegation Discovery System) per convertire un valore in un altro valore o per sostituire un valore con un altro. Ad esempio, un uso comune è quello di convertire i numeri di telefono in URIs SIP. Per ulteriori informazioni, consulta Tipo di record NAPTR.
- Strumento di test di query DNS: ora puoi simulare le query DNS per un record e visualizzare il valore restituito da Route 53. Per i record di geolocalizzazione e latenza, puoi anche simulare le richieste provenienti da un particolare indirizzo IP del resolver DNS. and/or client IP address to find out what response Route 53 would return to a client with that resolver and/or Per ulteriori informazioni, consulta Verifica delle risposte DNS da Route 53.

11 agosto 2016

Con questa versione puoi creare record alias che instradano il traffico verso Application Load Balancer ELB. Il processo è lo stesso per i Classic Load Balancer. Per ulteriori informazioni, consulta Valore/instradamento traffico a.

9 agosto 2016

Con questo rilascio, Route 53 aggiunge il supporto per DNSSEC per la registrazione dei domini. DNSSEC consente di proteggere il dominio dagli attacchi di spoofing DNS, noti anche come attacchi. man-in-the-middle Per ulteriori informazioni, consulta Configurazione di DNSSEC per un dominio.

7 luglio 2016

Puoi ora estendere manualmente la registrazione per un dominio e registrare un dominio con un periodo di registrazione iniziale più lungo del periodo di registrazione minimo specificato dal record. Per ulteriori informazioni, consulta Estendere il periodo di registrazione per un dominio.

6 luglio 2016

Se sei un cliente AISPL con un indirizzo di contatto in India, puoi ora utilizzare Route 53 per registrare domini. Per ulteriori informazioni, consulta la pagina relativa alla gestione di un account in India.

26 maggio 2016

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Report di fatturazione del dominio: ora puoi scaricare un report che elenca tutte le tariffe di registrazione del dominio, in base al dominio, per un periodo di tempo specificato. Il rapporto

include tutte le operazioni di registrazione dei domini per le quali è prevista una tariffa, tra cui la registrazione di domini, il trasferimento di domini su Route 53, il rinnovo della registrazione del dominio e (per alcune) la modifica del proprietario di un dominio. TLDs Per ulteriori informazioni, consulta la seguente documentazione :

- Console Route 53: consulta Download di un report di fatturazione domini
- API Route 53: consulta la ViewBillingpagina di riferimento dell'API Amazon Route 53.

- Novità TLDs: ora puoi registrare domini con quanto segue TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website e .uk. Per ulteriori informazioni, consulta Domini che è possibile registrare con Amazon Route 53.
- Novità APIs per la registrazione del dominio: per le operazioni che richiedono la conferma della validità dell'indirizzo e-mail del contatto del registrante, come la registrazione di un nuovo dominio, ora puoi determinare a livello di codice se il contatto del registrante ha fatto clic sul link nell'e-mail di conferma e, in caso contrario, se il link è ancora valido. È anche possibile richiederci in modo programmatico di inviare un'altra e-mail di conferma. Per ulteriori informazioni, consulta la documentazione seguente nella Documentazione di riferimento delle API di Amazon Route 53:
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

5 aprile 2016

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Controlli sanitari basati su CloudWatch metriche: ora puoi creare controlli sanitari basati sullo stato di allarme di qualsiasi CloudWatch metrica. Questa funzione è utile per controllare l'integrità degli endpoint che non possono essere raggiunti da un controllo dell'integrità di Route 53 standard, ad esempio le istanze all'interno di un Amazon Virtual Private Cloud (VPC) che dispongono solo di indirizzi IP privati. Per ulteriori informazioni, consulta la seguente documentazione :
  - Console Route 53: consulta Monitoraggio di un allarme CloudWatch nell'argomento "Valori che specifichi durante la creazione o l'aggiornamento di controlli dell'integrità".
  - API Route 53: consulta CreateHealthCheck e UpdateHealthCheckconsulta il riferimento all'API Amazon Route 53.
- Percorsi di controllo dell'integrità configurabili: ora puoi scegliere le regioni di controllo dell'integrità di Route 53 in grado di controllare l'integrità delle tue risorse, funzione che riduce il carico sull'endpoint dovuto ai controlli dell'integrità. Questa funzione è utile se i tuoi clienti sono

concentrato in una o più regioni geografiche. Per ulteriori informazioni, consulta la seguente documentazione :

- Console Route 53: consulta Configurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint)) nell'argomento "Valori che specifichi durante la creazione o l'aggiornamento di controlli dell'integrità".
- API Route 53: consulta l'`Regions`elemento per CreateHealthCheck e UpdateHealthChecknel riferimento all'API di riferimento di Amazon Route 53.

- Failover in zone ospitate private: ora puoi creare record di failover e record alias di failover in una zona ospitata privata. Quando si combina questa caratteristica con i controlli dell'integrità basati su parametri, è possibile configurare il failover DNS anche per gli endpoint che dispongono solo di indirizzi IP privati e non possono essere raggiunti utilizzando controlli dell'integrità di Route 53 standard. Per ulteriori informazioni, consulta la seguente documentazione :
  - Console Route 53: consulta Configurazione del failover in una zona ospitata privata.
  - API Route 53: consulta la ChangeResourceRecordSetspagina di riferimento dell'API Amazon Route 53.
- Record di alias in zone ospitate private: in passato potevi creare record alias DNS per instradare le query DNS solo ad altri record Route 53 nella stessa zona ospitata. Con questa versione, puoi anche creare record alias per instradare le query DNS ad ambienti Elastic Beanstalk con sottodomini regionalizzati, bilanciatori del carico di Elastic Load Balancing e bucket Amazon S3. (Non è ancora possibile creare record di alias che indirizzino le query DNS a una CloudFront distribuzione). Per ulteriori informazioni, consulta la seguente documentazione :
  - Console Route 53: consulta Scelta tra record alias e non alias.
  - API Route 53: consulta la ChangeResourceRecordSetspagina di riferimento dell'API Amazon Route 53.

23 febbraio 2016

Quando crei o aggiorni i controlli dell'integrità HTTPS, ora puoi configurare Route 53 per inviare il nome host all'endpoint durante la negoziazione TLS. Ciò consente all'endpoint di rispondere alla richiesta HTTPS con il certificato SSL/TLS applicabile. Per ulteriori informazioni, vedere la descrizione dello SNI nel Configurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint)) campo nell'argomento «Valori specificati quando si creano o si aggiornano i controlli sanitari». Per informazioni su come abilitare SNI quando utilizzi l'API per creare o aggiornare un

controllo dello stato, consulta CreateHealthCheck e UpdateHealthCheck nel riferimento all'API di riferimento di Amazon Route 53.

27 gennaio 2016

Ora puoi registrare domini per oltre 100 domini di primo livello aggiuntivi (TLDs) come .accountants, .band e .city. Per un elenco completo di quelli supportati, consulta. TLDs Domini che è possibile registrare con Amazon Route 53

19 gennaio 2016

Ora puoi creare record alias che instradano il traffico verso ambienti Elastic Beanstalk. Per informazioni sulla creazione di record utilizzando la console Route 53, consulta Creazione di record utilizzando la console Amazon Route 53. Per informazioni sull'utilizzo dell'API per creare record, consulta ChangeResourceRecordSetsAmazon Route 53 API Reference.

Versioni 2015

3 dicembre 2015

La console Route 53 ora include un editor visivo che ti consente di creare rapidamente complesse configurazioni di routing che utilizzano una combinazione di policy di routing ponderate, di latenza, di failover e di geolocalizzazione di Route 53. Puoi quindi associare la configurazione a uno o più nomi di dominio (ad esempio esempio.com) o nomi di sottodominio (ad esempio www.esempio.com), nella stessa zona ospitata o in più hosted zone. Inoltre, puoi eseguire il roll back degli aggiornamenti se la nuova configurazione non offre le prestazioni previste. La stessa funzionalità è disponibile utilizzando l'API Route 53 AWS SDKs, AWS CLI, e AWS Tools for Windows PowerShell. Per ulteriori informazioni sull'utilizzo dell'editor visivo, consulta Utilizzo di Traffic Flow per instradare il traffico DNS. Per informazioni su come utilizzare l'API per creare configurazioni di flusso del traffico, consulta la Documentazione di riferimento delle API di Amazon Route 53.

19 ottobre 2015

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Registrazione di domini per domini.com e.net da parte di Amazon Registrar, Inc. — Amazon è ora un registrar accreditato da ICANN per i domini di primo livello.com e.net () TLDs tramite Amazon Registrar, Inc. Quando utilizzi Route 53 per registrare un dominio.com o.net, Amazon Registrar sarà il registrar registrato e verrà indicato come «Registrar sponsor» nei risultati

della tua query Whois. Per informazioni sull'utilizzo di Route 53 per la registrazione dei domini, consulta Come registrare e gestire domini tramite Amazon Route 53.

- Protezione della privacy per domini .com e .net: quando record un dominio .com o .net con Route 53, tutte le tue informazioni personali, compresi nome e cognome, ora sono nascoste. Nome e cognome non sono nascosti per altri domini che record con Route 53. Per ulteriori informazioni sulla protezione della privacy, consulta Abilitazione o disabilitazione della protezione della privacy per le informazioni di contatto per un dominio.

15 settembre 2015

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Controlli dell'integrità calcolati: ora puoi creare controlli dell'integrità il cui stato viene determinato dallo stato di integrità di altri controlli dell'integrità. Per ulteriori informazioni, consulta Creazione e aggiornamento di controlli dell'integrità. Inoltre, consulta il riferimento CreateHealthCheckalle API di Amazon Route 53.
- Misurazioni di latenza per i controlli dell'integrità: ora puoi configurare Route 53 per misurare la latenza tra gli strumenti di controllo dell'integrità e il tuo endpoint. I dati sulla latenza vengono visualizzati nei CloudWatch grafici di Amazon nella console Route 53. Per abilitare le misurazioni di latenza per nuovi controlli dell'integrità, consulta l'impostazione Latency measurements (Misurazioni di latenza) in Configurazione avanzata (solo "Monitor an endpoint" (Monitora un endpoint)) nell'argomento Valori che specifichi durante la creazione o l'aggiornamento dei controlli dell'integrità. (Non è possibile abilitare misurazioni di latenza per controlli dell'integrità esistenti.) Inoltre, consulta MeasureLatencyl'argomento CreateHealthChecknel riferimento alle API di Amazon Route 53.
- Aggiornamenti alla dashboard per i controlli di integrità nella console Route 53: la dashboard per il monitoraggio dei controlli di integrità è stata migliorata in diversi modi, inclusi CloudWatch grafici per il monitoraggio della latenza tra i controllori dello stato di Route 53 e gli endpoint. Per ulteriori informazioni, consulta Monitoraggio dello stato del controllo dell'integrità e ricezione di notifiche.

3 marzo 2015

La Guida per gli sviluppatori di Amazon Route 53 ora spiega come configurare i server dei nomi white label per le zone ospitate di Route 53. Per ulteriori informazioni, consulta Configurazione dei server di nomi white label.

26 febbraio 2015

Ora puoi utilizzare l'API Route 53 per elencare le zone ospitate associate a un AWS account in ordine alfabetico per nome. È inoltre possibile ottenere un conteggio delle zone ospitate che sono associate a un account. Per ulteriori informazioni, consulta ListHostedZonesByNamee GetHostedZoneCountconsulta Amazon Route 53 API Reference.

11 febbraio 2015

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- Stato del controllo dell'integrità: la pagina dei controlli dell'integrità nella console Route 53 ora include una colonna Stato che ti consente di visualizzare lo stato globale di tutti i tuoi controlli dell'integrità. Per ulteriori informazioni, consulta Visualizzazione dello stato del controllo dell'integrità e motivo degli errori del controllo dell'integrità.
- Integrazione con AWS CloudTrail — Route 53 ora consente CloudTrail di acquisire informazioni su ogni richiesta che il tuo AWS account invia all'API Route 53. L'integrazione di Route 53 CloudTrail consente di determinare quali richieste sono state fatte all'API Route 53, l'indirizzo IP di origine da cui è stata effettuata ogni richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altro ancora. Per ulteriori informazioni, consulta Registrazione delle chiamate API Amazon Route 53 con AWS CloudTrail.
- Allarmi rapidi per controlli sanitari: quando crei un controllo dello stato utilizzando la console Route 53, ora puoi creare contemporaneamente un CloudWatch allarme Amazon per il controllo dello stato e specificare a chi inviare una notifica quando Route 53 ritiene che l'endpoint non sia integro per un minuto. Per ulteriori informazioni, consulta Creazione e aggiornamento di controlli dell'integrità.
- Assegnazione di tag per zone ospitate e domini: ora puoi assegnare i tag, che in genere vengono utilizzati per l'allocazione dei costi, ai domini e alle zone ospitate di Route 53. Per ulteriori informazioni, consulta Assegnazione di tag alle risorse di Amazon Route 53.

5 febbraio 2015

È ora possibile utilizzare la console Route 53 per aggiornare le informazioni di contatto per un dominio. Per ulteriori informazioni, consulta Valori specificati durante la registrazione o il trasferimento di un dominio.

22 gennaio 2015

Ora puoi specificare i nomi di dominio internazionalizzati durante la registrazione di un nuovo nome di dominio con Route 53. (Route 53 già supportava i nomi di dominio internazionalizzati per zone ospitate e record.) Per ulteriori informazioni, consulta Formato del nome dominio DNS.

Versioni 2014

25 novembre 2014

Con questa versione, è ora possibile modificare il commento specificato per una zona ospitata al momento della creazione. Nella console, è sufficiente fare clic sull'icona a forma di matita accanto al campo Comment (Commento) e immettere un nuovo valore. Per ulteriori informazioni sulla modifica del commento utilizzando l'API Route 53, consulta UpdateHostedZoneCommentAmazon Route 53 API Reference.

5 novembre 2014

Con questo rilascio, Route 53 aggiunge le seguenti nuove funzionalità:

- DNS privato VPCs creato utilizzando il servizio Amazon Virtual Private Cloud: ora puoi usare Route 53 per gestire i tuoi nomi di dominio interni VPCs senza esporre i dati DNS alla rete Internet pubblica. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.
- Motivi di errore dei controlli dell'integrità: ora puoi consultare lo stato corrente di un controllo dell'integrità selezionato, nonché i dettagli sul motivo dell'errore dell'ultimo controllo dell'integrità, come riportato da ciascuno degli strumenti di controllo dell'integrità di Route 53. Lo stato include il codice di stato HTTP e i motivi di errore includono informazioni sui vari tipi di errori, come errori di corrispondenza stringa e timeout di risposta. Per ulteriori informazioni, consulta Visualizzazione dello stato del controllo dell'integrità e motivo degli errori del controllo dell'integrità.
- Set di delega riutilizzabili: ora puoi applicare lo stesso set di quattro server dei nomi ufficiali, noti collettivamente come un set di delega, a più zone ospitate corrispondenti a diversi nomi di dominio. Questo semplifica notevolmente il processo di migrazione del servizio DNS a Route 53 e la gestione di un numero elevato di zone ospitate. Per l'utilizzo di set di delega riutilizzabili, al momento è necessario utilizzare l'API Route 53 o un SDK AWS . Per ulteriori informazioni, consulta il riferimento API di Amazon Route 53.
- Routing di geolocalizzazione migliorato: abbiamo ulteriormente migliorato la precisione del routing di geolocalizzazione aggiungendo il supporto per l'estensione di EDNS0. edns-client-subnet Per ulteriori informazioni, consulta Routing di geolocalizzazione.
- Supporto per Signature v4: ora puoi effettuare l'accesso a tutte le richieste API di Route 53 utilizzando Signature versione 4. Per ulteriori informazioni, consulta Firma delle richieste dell'API Route 53 nella Documentazione di riferimento delle Api di Amazon Route 53.

31 luglio 2014

Con questa versione, ora puoi:

- Registra i nomi di dominio tramite Route 53. Per ulteriori informazioni, consulta Come registrare e gestire domini tramite Amazon Route 53.
- Configura Route 53 per rispondere alle query DNS in base alla posizione geografica da cui provengono. Per ulteriori informazioni, consulta Routing di geolocalizzazione.

2 luglio 2014

Con questa versione, ora puoi:

- Modificare la maggior parte dei valori nei controlli dell'integrità. Per ulteriori informazioni, consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.
- Utilizza l'API di Route 53 per ottenere un elenco di tutti gli intervalli di indirizzi IP che gli strumenti di controllo dell'integrità di Route 53 utilizzano per controllare l'integrità delle risorse. È possibile utilizzare questi indirizzi IP per configurare il router e le regole del firewall per consentire agli strumenti di controllo dell'integrità di controllare lo stato delle risorse. Per ulteriori informazioni, GetCheckerIpRangesconsulta Amazon Route 53 API Reference.
- Assegnare tag per l'allocazione dei costi a controlli dell'integrità, che consente anche di assegnare un nome ai controlli dell'integrità. Per ulteriori informazioni, consulta Denominazione e tagging di controlli dell'integrità.
- Usa l'API Route 53 per ottenere il numero di controlli sanitari associati al tuo AWS account. Per ulteriori informazioni, GetHealthCheckCountconsulta Amazon Route 53 API Reference.

30 aprile 2014

Con questa versione, è ora possibile creare controlli dell'integrità e utilizzare un nome di dominio invece di un indirizzo IP per specificare l'endpoint. Ciò è utile quando l'indirizzo IP di un endpoint non è fisso o è servito da più istanze IPs, come Amazon EC2 o Amazon RDS. Per ulteriori informazioni, consulta Creazione e aggiornamento di controlli dell'integrità.

Inoltre, alcune informazioni sull'utilizzo dell'API Route 53 che precedentemente erano riportate nella Guida per gli sviluppatori di Amazon Route 53 sono state spostate. Ora tutta le documentazione relativa all'API è riportata nella Documentazione di riferimento delle API di Amazon Route 53.

18 aprile 2014

Con questo rilascio, Route 53 passa un valore diverso nell'intestazione `Host` quando il valore di Porta del controllo dell'integrità è 443 e il valore di Protocollo è HTTPS. Durante un controllo

dell'integrità, Route 53 ora passa all'endpoint una intestazione `Host` contenente il valore del campo Nome host. Se è stato creato il controllo dell'integrità utilizzando l'operazione API `CreateHealthCheck`, questo è il valore dell'elemento `FullyQualifiedDomainName`.

Per ulteriori informazioni, consulta Creazione, aggiornamento ed eliminazione dei controlli dell'integrità.

9 aprile 2014

Con questo rilascio, è ora possibile visualizzare la percentuale di strumenti di controllo dell'integrità di Route 53 che attualmente segnalano che un endpoint è integro.

Inoltre, il comportamento della metrica Health Check Status in Amazon CloudWatch ora mostra solo zero (se l'endpoint non era integro durante un determinato periodo di tempo) o uno (se l'endpoint era integro per quel periodo di tempo). Il parametro non mostra valori tra 0 e 1 che riflettono la porzione dei controlli dell'integrità di Route 53 che segnalano che l'endpoint è integro.

Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

18 febbraio 2014

Con questo rilascio, Route 53 aggiunge le seguenti funzionalità:

- Soglia di failover del controllo dell'integrità: ora puoi specificare il numero di controlli dell'integrità consecutivi per cui un endpoint deve avere esito negativo prima che Route 53 consideri l'endpoint non integro (numero compreso tra 1 e 10). Un endpoint non integro dovrà superare lo stesso numero di controlli per essere considerato integro. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.
- Intervallo di richiesta del controllo dell'integrità: ora puoi specificare la frequenza con la quale Route 53 deve inviare le richieste a un endpoint per determinare se l'endpoint è integro. Le impostazioni valide sono 10 secondi e 30 secondi. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

30 gennaio 2014

Con questo rilascio, Route 53 aggiunge le seguenti funzionalità:

- Controlli dell'integrità con corrispondenza stringa HTTP e HTTPS: Route 53 supporta ora controlli dell'integrità in grado di determinare l'integrità di un endpoint in base all'aspetto di una stringa specificata nel corpo della risposta. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

- Controlli dell'integrità HTTPS: Route 53 supporta ora controlli dell'integrità per siti Web sicuri, solo SSL. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.
- **`UPSERT`** per l'operazione API **`ChangeResourceRecordSets`**: durante la creazione o la modifica di record utilizzando l'operazione API `ChangeResourceRecordSets`, ora puoi utilizzare l'operazione `UPSERT` per creare un nuovo record se non ne esiste alcuno con un determinato nome e tipo, o per aggiornare un record esistente. Per ulteriori informazioni, ChangeResourceRecordSetsconsulta Amazon Route 53 API Reference.

7 gennaio 2014

Con questo rilascio, Route 53 aggiunge il supporto per i controlli dell'integrità in grado di determinare l'integrità di un endpoint in base al fatto che una stringa specificata viene visualizzata o meno nel corpo della risposta. Per ulteriori informazioni, consulta Come Amazon Route 53 determina se un controllo dell'integrità è integro.

Versioni 2013

14 agosto 2013

Con questo rilascio, Route 53 aggiunge il supporto per la creazione di record importando un file di zona in formato BIND. Per ulteriori informazioni, consulta Creazione di record mediante importazione di un file di zona.

Inoltre, le CloudWatch metriche per i controlli dello stato di Route 53 sono state integrate nella console Route 53 e semplificate. Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

26 giugno 2013

Con questa versione, Route 53 aggiunge il supporto per l'integrazione dei controlli sanitari con le CloudWatch metriche, in modo da poter effettuare le seguenti operazioni:

- Verificare che un controllo dell'integrità sia configurato correttamente.
- Esaminare lo stato di un endpoint di controllo dell'integrità in un periodo di tempo specificato.
- Configura CloudWatch l'invio di un avviso Amazon Simple Notification Service (Amazon SNS) quando tutti gli addetti al controllo dello stato di Route 53 ritengono che l'endpoint specificato non sia integro.

Per ulteriori informazioni, consulta Monitoraggio dei controlli sanitari tramite CloudWatch.

11 giugno 2013

Con questa versione, Route 53 aggiunge il supporto per la creazione di record di alias che indirizzano le query DNS verso nomi di dominio alternativi per le distribuzioni Amazon. CloudFront Puoi utilizzare questa funzione sia per i nomi di dominio alternativi dall'apex di zona (esempio.com) sia i nomi di dominio alternativi per i sottodomini (www.esempio.com). Per ulteriori informazioni, consulta Instradamento del traffico verso una CloudFront distribuzione Amazon utilizzando il tuo nome di dominio.

30 maggio 2013

Con questa versione, Route 53 aggiunge il supporto per la valutazione dello stato dei sistemi di bilanciamento del carico ELB e delle istanze Amazon associate. EC2 Per ulteriori informazioni, consulta Creazione di controlli sanitari su Amazon Route 53 .

28 marzo 2013

La documentazione sui controlli dell'integrità e di failover è stata riscritta per migliorare la fruibilità. Per ulteriori informazioni, consulta Creazione di controlli sanitari su Amazon Route 53 .

11 febbraio 2013

Con questo rilascio, Route 53 aggiunge il supporto per il failover e i controlli dell'integrità. Per ulteriori informazioni, consulta Creazione di controlli sanitari su Amazon Route 53 .

Versione 2012

21 marzo 2012

Con questa versione, Route 53 consente di creare record di latenza. Per ulteriori informazioni, consulta Routing basato sulla latenza.

Versioni 2011

21 dicembre 2011

Con questa versione, la console Route 53 AWS Management Console consente di creare un record di alias scegliendo un Elastic Load Balancer da un elenco anziché inserire manualmente l'ID della zona ospitata e il nome DNS del load balancer. Le nuove funzionalità sono documentate nella Guida per gli sviluppatori di Amazon Route 53.

16 novembre 2011

Con questa versione, è possibile utilizzare la console Route 53 AWS Management Console per creare ed eliminare zone ospitate e per creare, modificare ed eliminare record. Le nuove funzionalità sono documentate nella Guida per gli sviluppatori di Amazon Route 53, come pertinente.

18 ottobre 2011

La Guida alle operazioni di base di Amazon Route 53 è stata unita con la Guida per gli sviluppatori di Amazon Route 53 e la Guida per gli sviluppatori è stata riorganizzata per migliorarne l'usabilità.

24 maggio 2011

Questo rilascio di Amazon Route 53 introduce record alias, che consentono di creare alias di apex di zona; record ponderati; una nuova API (2011-05-05); e un Accordo sul Livello di Servizio (SLA). Inoltre, dopo sei mesi in beta, Route 53 è ora disponibile al pubblico. Per ulteriori informazioni, consulta la pagina di Amazon Route 53 e Scelta tra record alias e non alias nella Guida per gli sviluppatori di Amazon Route 53.

Versione 2010

5 dicembre 2010

Questo è il primo rilascio della Guida per gli sviluppatori di Amazon Route 53.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.