aws

Guia do Desenvolvedor

Amazon Route 53

Versão da API 2013-04-01

Amazon Route 53: Guia do Desenvolvedor

Table of Contents

O que é o Amazon Route 53?

O Amazon Route 53 é um serviço da web do Sistema de Nomes de Domínio (DNS) altamente disponível e dimensionável. Você pode usar o Route 53 para executar três funções principais em qualquer combinação: registro de domínios, roteamento de DNS e verificação de integridade.

Se você optar por usar o Route 53 para todas as três funções, siga a ordem abaixo:

1. Registrar nomes de domínio

   Seu site precisa de um nome, como example.com. O Route 53 permite que você registre um nome para seu site ou aplicação Web, conhecido como um nome de domínio.

   - Para obter uma visão geral, consulte Como funciona o registro de domínio.
   - Para um procedimento, consulte Registrar um novo domínio.
   - Para um tutorial que descreve como registrar um domínio e criar um site simples em um bucket do Amazon S3, consulte Conceitos básicos do Amazon Route 53.

2. Rotear tráfego de Internet para os recursos do seu domínio

   Quando um usuário abre um navegador da Web e informa seu nome de domínio (example.com) ou nome de subdomínio (acme.example.com) na barra de endereços, o Route 53 ajuda a conectar o navegador com o site ou a aplicação Web.

   - Para obter uma visão geral, consulte Como o tráfego da Internet é roteado para seu site ou o aplicativo web.
   - Para ver os procedimentos, consulte Configurar o Amazon Route 53 como serviço DNS.
   - Para obter um procedimento sobre como encaminhar e-mails para a Amazon WorkMail, consulteRoteamento de tráfego para a Amazon WorkMail.

3. Verificar a integridade de seus recursos

   O Route 53 envia solicitações automáticas através da Internet a um recurso, como um servidor Web, para verificar se está acessível, disponível e funcional. Você também pode optar por receber notificações quando um recurso se tornar indisponível e optar por desviar o tráfego da Internet dos recursos não íntegros.

   - Para obter uma visão geral, consulte Como o Amazon Route 53 verifica a integridade dos seus recursos.
   - Para ver os procedimentos, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

Outros recursos do Route 53

Além de ser um serviço web de Sistema de Nomes de Domínio (DNS), o Route 53 oferece os seguintes recursos:

Route 53 Resolver

Obtenha DNS recursivo para suas Amazon VPCs em Regiões da AWS, VPCs em AWS Outposts racks ou qualquer outra rede local. Crie regras de encaminhamento condicional e endpoints do Route 53 para resolver nomes personalizados dominados em zonas hospedadas privadas do Route 53 ou em seus servidores DNS locais.

Para obter mais informações, consulte O que Amazon Route 53 Resolveré.

Resolver do Amazon Route 53 em endpoints do Outposts

Conecte o Route 53 Resolver em racks Outpost com servidores DNS em seus data centers locais por meio de endpoints do Route 53 Resolver. Isso permite a resolução de consultas de DNS entre os racks do Outposts e seus outros recursos locais.

Para obter mais informações, consulte O que é o Amazon Route 53 no Outposts?.

Firewall de DNS do Route 53 Resolver

Proteja suas consultas de DNS recursivas no Resolvedor do Route 53. Crie listas de domínios e crie regras de firewall que filtrem o tráfego DNS de saída em relação a essas regras.

Para obter mais informações, consulte Firewall de DNS do Route 53 Resolver.

Fluxo de tráfego

Gerenciamento global de tráfego eletrônico asy-to-use e econômico: direcione os usuários finais para o melhor endpoint para seu aplicativo com base na geoproximidade, latência, integridade e outras considerações.

Para obter mais informações, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS.

Perfis do Amazon Route 53

Com os Perfis do Route 53, você pode aplicar e gerenciar configurações do Route 53 relacionadas ao DNS em várias VPCs e em diferentes. Conta da AWS

Para obter mais informações, consulte Perfis do Amazon Route 53.

Tópicos

Como funciona o registro de domínio

Se você deseja criar um site ou um aplicativo web, comece registrando o nome do seu site, conhecido como domain name. O seu nome de domínio é o nome, como exemplo.com, que seus usuários inserem em um navegador para exibir o site.

Aqui está uma visão geral de como registrar um nome de domínio no Amazon Route 53:

1. Você escolhe um nome de domínio e confirma que ele está disponível, isto é, nenhuma outra pessoa registrou o nome de domínio que você quer.

   Se o nome de domínio desejado já está em uso, você pode experimentar outros nomes ou tentar alterar apenas o domínio de nível superior, como .com, para outro domínio de nível superior, como .ninja ou .hockey. Para obter uma lista dos domínios de nível superior para os quais o Route 53 oferece suporte, consulte Domínios que você pode registrar com o Amazon Route 53.
2. Você registra o nome de domínio com o Route 53. Ao registrar um domínio, você fornece nomes e informações de contato do proprietário do domínio e de outros contatos.

   Quando você registra um domínio com o Route 53, o serviço cria automaticamente o serviço de DNS para o domínio fazendo o seguinte:

   - Cria uma hosted zone que tenha o mesmo nome que o seu domínio.
   - Atribui um conjunto de quatro servidores de nome para a zona hospedada. Quando alguém usa um navegador para acessar seu site, como www.example.com, esses servidores de nome dizem ao navegador onde encontrar seus recursos, como um servidor Web ou um bucket do

Amazon S3. (O Amazon S3 é um armazenamento de objetos para armazenar e recuperar qualquer quantidade de dados em qualquer lugar na Web. Um bucket é um contêiner para objetos que você armazena no S3.)

- Obtém os servidores de nome da zona hospedada e os adiciona ao domínio.

Para ter mais informações, consulte Como o tráfego da Internet é roteado para seu site ou o aplicativo web.

3. No final do processo de registro, enviamos suas informações para o registrador do domínio. O domain registrar é o Amazon Registrar, Inc. ou nosso registrador associado, Gandi. Para saber quem é o registrador do seu domínio, consulte Como encontrar seu registrador.
4. O registrador envia suas informações para o registro do domínio. Um registro é uma empresa que vende registros de domínio para um ou mais domínios de nível superior, como .com.
5. O registro armazena as informações sobre o seu domínio em um banco de dados próprio além de armazenar algumas informações no banco de dados público WHOIS.

Para obter mais informações sobre como registrar um nome de domínio, consulte Registrar um novo domínio.

Se você já registrou um nome de domínio com outro registrador, pode optar por transferir o registro de domínio para o Route 53. Isso não é necessário para usar outros recursos do Route 53. Para ter mais informações, consulte Como transferir registro de um domínio para o Amazon Route 53.

Como o tráfego da Internet é roteado para seu site ou o aplicativo web

Todos os computadores conectados à Internet, desde o seu smartphone ou laptop aos servidores que oferecem conteúdo para sites pesados de varejo, se comunicam usando números. Esses números, conhecidos como endereços IP, estão em um dos seguintes formatos:

- Protocolo de Internet versão 4 (IPv4), como 192.0.2.44
- Protocolo de Internet versão 6 (IPv6), como 2001:0db8:85a3:0000:0000:abcd:0001:2345

Ao abrir um navegador e acessar um site, você não precisa lembrar e digitar uma string de caracteres longa como essa. Em vez disso, você pode digitar um nome de domínio como example.com e ainda chegar ao lugar certo. Um serviço de DNS, como o Amazon Route 53, ajuda a fazer essa conexão entre nomes de domínio e endereços IP.

Tópicos

Visão geral de como configurar o Amazon Route 53 para encaminhar o tráfego da Internet para seu domínio

Esta é uma visão geral de como usar o console do Amazon Route 53 para registrar um nome de domínio e configurar o Route 53 para encaminhar o tráfego da Internet para seu site ou aplicação Web.

1. Registre o nome de domínio que você deseja que os usuários usem para acessar seu conteúdo. Para obter uma visão geral, consulte Como funciona o registro de domínio.
2. Depois de registrar o seu nome de domínio, o Route 53 cria automaticamente uma zona hospedada pública que tem o mesmo nome do domínio. Para ter mais informações, consulte Trabalhar com zonas hospedadas públicas.
3. Para rotear o tráfego para seus recursos, você cria registros, também conhecidos como conjuntos de registros de recursos em sua zona hospedada. Cada registro inclui informações sobre como você deseja rotear o tráfego para seu domínio, como o seguinte:

   Nome

   O nome do registro corresponde ao nome de domínio (example.com) ou subdomínio (www.example.com, retail.example.com) para o qual você deseja que o Route 53 encaminhe o tráfego.

   O nome de cada registro em uma zona hospedada deve terminar com o nome da zona hospedada. Por exemplo, se o nome da zona hospedada é exemplo.com, todos os nomes de registro devem terminar em exemplo.com. O console do Route 53 faz isso para você automaticamente.

   Type (Tipo)

   O tipo de registro geralmente determina o tipo de recurso para o qual você deseja que o tráfego seja roteado. Por exemplo, para rotear tráfego para um servidor de e-mail, especifique MX como o tipo. Para rotear o tráfego para um servidor web com um endereço IP IPv4, você especifica o Tipo como A.

Value (Valor)

O Valor é intimamente ligado ao Tipo. Se você especifica o Tipo como MX, especifica os nomes de um ou mais servidores de e-mail como Valor. Se você especificar o Tipo como A, especifica um endereço IP no formato IPv4, como 192.0.2.136.

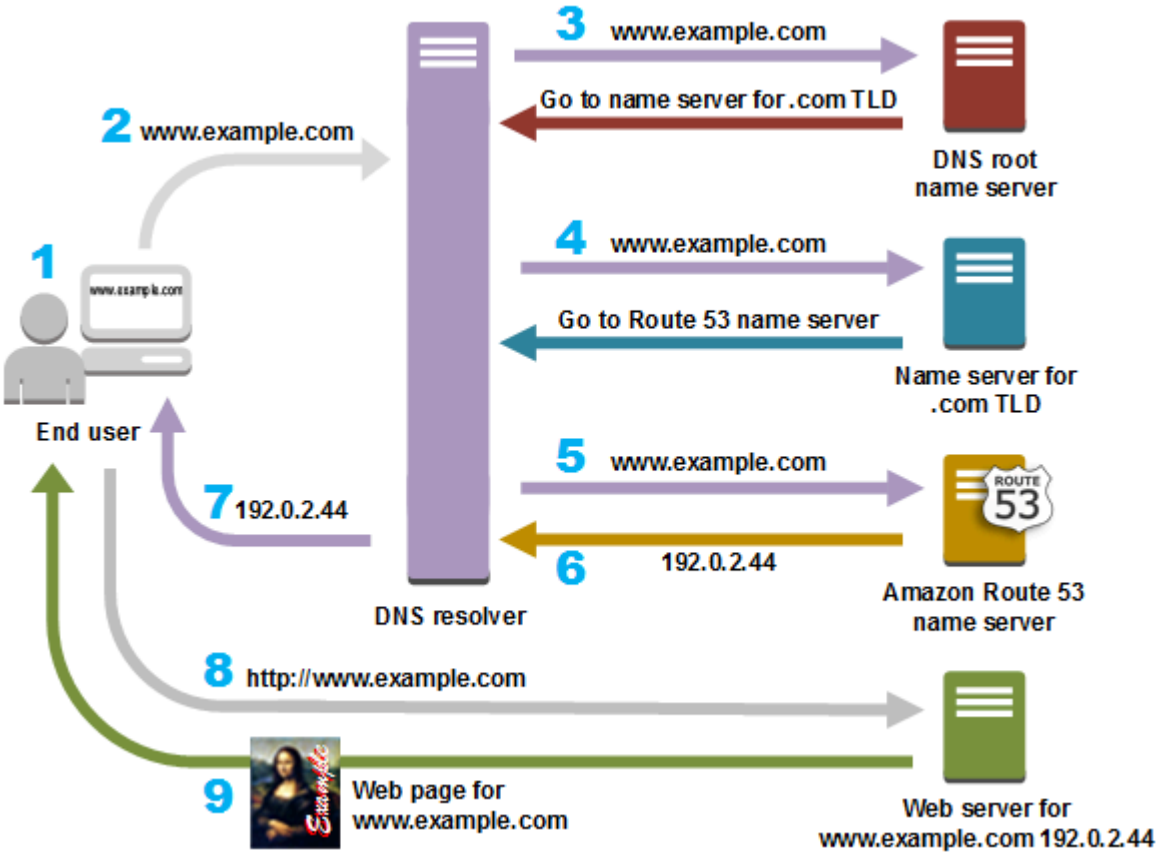
Para obter mais informações sobre registros de , consulte Trabalhar com registros.

Você também pode criar registros especiais do Route 53, chamados de registros de alias, que direcionam o tráfego para buckets do Amazon S3, distribuições CloudFront da Amazon e outros recursos. AWS Para obter mais informações, consulte Escolher entre registros de alias e não alias e Encaminhando o tráfego da Internet para seus recursos AWS.

Para obter mais informações sobre o roteamento de tráfego de Internet para seus recursos, consulte Configurar o Amazon Route 53 como serviço DNS.

Como o Amazon Route 53 encaminha tráfego para o seu domínio

Depois de configurar o Amazon Route 53 para encaminhar o tráfego da Internet para seus recursos, como servidores Web ou buckets do Amazon S3, veja o que acontece em apenas alguns milissegundos quando alguém solicita conteúdo de www.example.com:



1. O usuário abre o navegador da Web, digita www.exemplo.com na barra de endereços e pressiona Enter.
2. A solicitação de www.exemplo.com é roteada para um resolvedor de DNS, que costuma ser gerenciado pelo provedor de serviço de Internet (ISP), como um provedor de Internet a cabo, um provedor de banda larga DSL ou uma rede corporativa.
3. O resolvedor de DNS do ISP encaminha a solicitação de example.com para um servidor de nome raiz DNS.
4. O resolvedor de DNS encaminha a solicitação de www.example.com novamente, desta vez para um dos servidores de nome TLD dos domínios .com. O servidor de nome dos domínios .com responde à solicitação com os nomes dos quatro servidores de nome do Route 53 associados ao domínio example.com.

   O resolvedor DNS armazena em cache os quatro servidores de nome do Route 53. Na próxima vez que alguém acessar exemplo.com, o resolvedor ignorará as etapas 3 e 4, pois ele já tem os servidores de nomes para exemplo.com. Os servidores de nome são normalmente armazenados em cache por dois dias.

5. O resolvedor de DNS escolhe um servidor de nome do Route 53 e encaminha a solicitação de www.example.com para esse servidor de nome.
6. O servidor de nome do Route 53 procura o registro www.example.com na zona hospedada example.com, obtém o valor associado, como o endereço IP de um servidor Web, 192.0.2.44, e retorna o endereço IP para o resolvedor do DNS.
7. O resolvedor de DNS finalmente tem o endereço IP de que o usuário precisa. O resolvedor retorna o valor para o navegador da web.

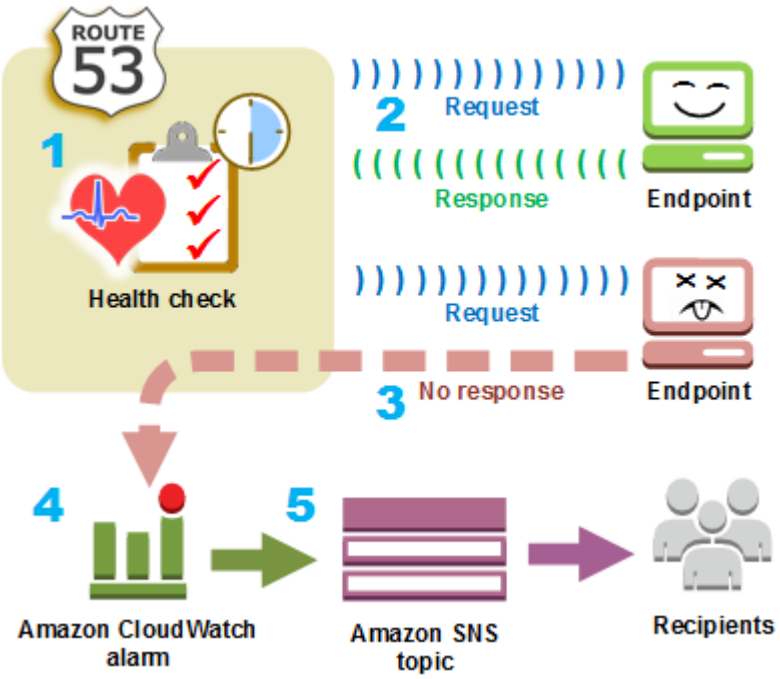
> **Note**
>
> O resolvedor de DNS também armazena em cache o endereço IP de exemplo.com por um período que você especificar. Assim, ele pode responder mais rapidamente na próxima vez que alguém acessar exemplo.com. Para ter mais informações, consulte time to live (TTL).

8. O navegador da Web envia uma solicitação de example.com para um endereço IP que ele obteve do resolvedor de DNS. Este é o lugar onde está o seu conteúdo. Por exemplo, um servidor Web em execução em uma instância do Amazon EC2 ou em um bucket do Amazon S3 que está configurado como um endpoint do site.
9. O servidor web ou outro recurso em 192.0.2.44 retorna a página da web de www.exemplo.com para o navegador da web e o navegador exibe a página.

Como o Amazon Route 53 verifica a integridade dos seus recursos

As verificações de integridade do Amazon Route 53 monitoram a integridade dos seus recursos, como servidores Web e servidores de e-mail. Opcionalmente, você pode configurar CloudWatch alarmes da Amazon para suas verificações de saúde, para receber uma notificação quando um recurso ficar indisponível.

Aqui está uma visão geral de como a verificação de integridade funciona se quiser ser notificado quando um recurso se tornar indisponível:



1. Você cria uma verificação de integridade e especifica os valores que definem como deseja que a verificação funcione, como o seguinte:
   - O endereço IP ou nome de domínio do endpoint, como um servidor Web, que você deseja que o Route 53 monitore. (Você também pode monitorar o status de outras verificações de saúde ou o estado de um CloudWatch alarme.)
   - O protocolo que você deseja que o Amazon Route 53 use para realizar a verificação: HTTP, HTTPS ou TCP.
   - Com que frequência você deseja que o Route 53 envie uma solicitação ao endpoint. Este é o intervalo de solicitação.
   - Quantas vezes consecutivas o endpoint deve deixar de responder às solicitações para que o Route 53 não o considere íntegro. Este é o limite de falha.
   - Opcionalmente, como você deseja ser notificado quando o Route 53 detecta que o endpoint está com problemas. Quando você configura a notificação, o Route 53 define automaticamente um CloudWatch alarme. CloudWatch usa o Amazon SNS para notificar os usuários de que um endpoint não está íntegro.
2. O Route 53 começa a enviar solicitações para o endpoint no intervalo especificado na verificação de integridade.

   Se o endpoint responde às solicitações, o Route 53 o considera íntegro e não toma qualquer medida.

3. Se o endpoint não responde a uma solicitação, o Route 53 começa a contabilizar o número de solicitações consecutivas a que o endpoint não responde:
   - Se a contagem atingir o valor que você especificou como o limite de falha, o Route 53 considera que o endpoint não está íntegro.
   - Se o endpoint começar a responder novamente antes que a contagem atinja o limite de falha, o Route 53 redefinirá a contagem para 0 e CloudWatch não entrará em contato com você.
4. Se o Route 53 considerar que o endpoint não está íntegro e se você configurou a notificação para a verificação de saúde, o Route 53 notificará. CloudWatch

   Se você não tiver configurado uma notificação, ainda poderá ver o status das verificações de integridade do Route 53 no console do Route 53. Para ter mais informações, consulte Monitorar o status da verificação de integridade e receber notificações.
5. Se você configurou a notificação para a verificação de saúde, CloudWatch aciona um alarme e usa o Amazon SNS para enviar a notificação aos destinatários especificados.

Além de verificar a integridade de um endpoint especificado, você pode configurar uma verificação de integridade para avaliar o estado de uma ou mais outras verificações de integridade, de modo que você pode ser notificado quando um número específico de recursos, como dois de cinco servidores web, estão indisponíveis. Você também pode configurar uma verificação de saúde para verificar o status de um CloudWatch alarme para que você possa ser notificado com base em uma ampla variedade de critérios, não apenas se um recurso está respondendo às solicitações.

Se você tem vários recursos que executam a mesma função, por exemplo, servidores Web ou servidores de banco de dados, e deseja que o Route 53 encaminhe o tráfego apenas para os recursos que estão íntegros, pode configurar o failover de DNS associando uma verificação de integridade a cada registro para esse recurso. Se uma verificação de integridade determinar que o recurso subjacente não está íntegro, o Route 53 desviará o tráfego do registro associado.

Para obter mais informações sobre o uso do Route 53 para monitorar a integridade dos recursos, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

Conceitos do Amazon Route 53

Aqui está uma visão geral dos conceitos discutidos por todo o Guia do desenvolvedor do Amazon Route 53.

Tópicos

- Conceitos de registro de domínio
- Conceitos de Domain Name System (DNS)
- Conceitos de planos de dados e de controle
- Conceitos de verificação de integridade

Conceitos de registro de domínio

Aqui está uma visão geral dos conceitos relacionados ao registro de domínio.

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

nome de domínio

O nome, como exemplo.com, que um usuário digita na barra de endereços de um navegador da web para acessar um site ou um aplicativo web. Para que o seu site ou aplicativo web fique disponível na Internet, você começa registrando um nome de domínio. Para ter mais informações, consulte Como funciona o registro de domínio.

registrador de domínios

Uma empresa credenciada pela ICANN (Internet Corporation for Assigned Names and Numbers) para processar registros de domínio para domínios de nível superior (TLDs) específicos. Para encontrar o registrador do seu domínio, consulte Como encontrar seu registrador.

registro de domínio

Uma empresa que tem o direito de vender domínios que têm um determinado domínio de nível superior. Por exemplo, VeriSigné o registro que possui o direito de vender domínios que tenham um TLD.com. Um registro de domínio define as regras para registrar um domínio, como requisitos de residência de um TLD geográfico. Um registro de domínio também mantém o banco de dados autoritativo para todos os nomes de domínio que têm o mesmo TLD. O banco de dados do registro contém informações, como informações de contato e os servidores de nome de cada domínio.

revendedor de domínio

Uma empresa que vende nomes de domínio para os registradores, como o Amazon Registrar. O Amazon Route 53 é um revendedor de domínio do Amazon Registrar e do Gandi, nosso registrador associado.

domínio de nível superior (TLD)

A última parte de um nome de domínio, como .com, .org ou .ninja. Há dois tipos de domínios de nível superior:

Domínios genéricos de nível superior

Em geral, esses TLDs fornecem aos usuários uma ideia do que eles encontrarão no site. Por exemplo, os nomes de domínio que têm um TLD de .bike costumam ser associados a sites de empresas ou negócios de motocicletas ou bicicletas. Com algumas exceções, você pode usar qualquer TLD genérico que desejar. Assim, um clube de bicicletas poderia usar um TLD .hockey como nome de domínio.

Domínios geográficos de nível superior

Esses TLDs são associados a áreas geográficas, como países ou cidades. Alguns registros para TLDs geográficos têm requisitos de residência. Outros, como o the section called “.io (Território Britânico do Oceano Índico)”, permitem ou até mesmo incentivam o uso de um TLD genérico.

Para obter uma lista de TLDs que você pode usar ao registrar um nome de domínio no Route 53, consulte Domínios que você pode registrar com o Amazon Route 53.

Conceitos de Domain Name System (DNS)

Aqui está uma visão geral dos conceitos relacionados 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)

registro de alias

Um tipo de registro que você pode criar com o Amazon Route 53 para rotear o tráfego para AWS recursos como CloudFront distribuições da Amazon e buckets do Amazon S3. Para ter mais informações, consulte Escolher entre registros de alias e não alias.

servidor de nome autoritativo

Um servidor de nome que tem informações definitivas sobre uma parte do Domain Name System (DNS) e que responde às solicitações do resolvedor de DNS retornando as informações aplicáveis. Por exemplo, um servidor de nome autoritativo do domínio de nível superior (TLD) .com conhece os nomes dos servidores de nome de cada domínio .com registrado. Quando um servidor de nome autoritativo .com recebe uma solicitação de um resolvedor de DNS de exemplo.com, ele responde com os nomes dos servidores de nome do serviço de DNS do domínio exemplo.com.

Os servidores de nome do Route 53 são os servidores de nome autoritativos de cada domínio que usa o Route 53 como o serviço DNS. Os servidores de nome sabem como você deseja encaminhar o tráfego do seu domínio e subdomínios com base nos registros criados na zona hospedada do domínio. (Os servidores de nome do Route 53 armazenam as zonas hospedadas dos domínios que usam o Route 53 como o serviço de DNS.)

Por exemplo, se um servidor de nome do Route 53 recebe uma solicitação de www.example.com, ele encontra esse registro e retorna o endereço IP, como 192.0.2.33, que é especificado no registro.

Bloco CIDR

Um bloco CIDR é um intervalo IP usado com roteamento baseado em IP. No Route 53, você pode especificar blocos CIDR de /0 a /24 para IPv4 e de 0 a /48 para IPv6. Por exemplo, um bloco CIDR IPv4 /24 inclui 256 endereços IP contíguos. Você pode agrupar conjuntos de blocos CIDR (ou intervalos IP) em locais CIDR, que, por sua vez, são agrupados em coleções CIDR reutilizáveis.

consulta ao DNS

Normalmente, uma solicitação enviada por um dispositivo, como um computador ou um smartphone, ao Domain Name System (DNS) de um recurso associado a um nome de domínio. O exemplo mais comum de uma consulta de DNS é quando um usuário abre um navegador e digita o nome de domínio na barra de endereços. A resposta a uma consulta de DNS normalmente é o endereço IP associado a um recurso, como um servidor web. O dispositivo que iniciou a solicitação usa o endereço IP para se comunicar com o recurso. Por exemplo, um navegador pode usar o endereço IP para obter uma página da web a partir de um servidor web.

resolvedor de DNS

Um servidor DNS, muitas vezes gerenciado por um provedor de serviços de Internet (ISP), que atua como um intermediário entre as solicitações de usuários e os servidores de nome DNS. Quando você abre um navegador e insere um nome de domínio na barra de endereços, sua consulta vai primeiro para um resolvedor de DNS. O resolvedor se comunica com servidores de nome DNS para obter o endereço IP do recurso correspondente, como um servidor web. Um resolvedor de DNS é também conhecido como um servidor de nome recursivo porque envia solicitações para uma sequência de servidores de nome DNS autoritativo até receber a resposta (normalmente, um endereço IP) que ele retorna a um dispositivo do usuário, por exemplo, um navegador da web em um laptop.

Domain Name System (DNS)

Uma rede mundial de servidores que ajudam os computadores, smartphones, tablets e outros dispositivos habilitados para IP a se comunicar entre si. O Domain Name System converte nomes de fácil compreensão como exemplo.com em números, conhecidos como endereços IP, que permitem que os computadores se encontrem na Internet.

Consulte também IP address.

zona hospedada

Um contêiner para registros que incluem informações sobre como você deseja rotear o tráfego para um domínio (como exemplo.com) e todos os seus subdomínios (como www.exemplo.com, varejo.exemplo.com e seattle.contabilidade.exemplo.com). Uma zona hospedada tem o mesmo nome que o domínio correspondente.

Por exemplo, a zona hospedada de exemplo.com pode incluir um registro que tem informações sobre o tráfego de roteamento de www.exemplo.com para um servidor web que tem o endereço IP 192.0.2.243 e um registro que tem informações sobre e-mail de roteamento de exemplo.com para dois servidores de e-mail, mail1.exemplo.com e mail2.exemplo.com. Cada servidor de e-mail também exige seu próprio registro.

Consulte também record (DNS record).

endereço IP

Um número atribuído a um dispositivo na Internet, como um laptop, um smartphone ou um servidor Web, que permite que o dispositivo se comunique com outros dispositivos na Internet. Os endereços IP estão em um dos seguintes formatos:

- Protocolo de Internet versão 4 (IPv4), como 192.0.2.44
- Protocolo de Internet versão 6 (IPv6), como 2001:0db8:85a3:0000:0000:abcd:0001:2345

O Route 53 oferece suporte a endereços IPv4 e IPv6 para as seguintes finalidades:

- Você pode criar registros que têm um tipo A e endereços IPv4, ou um tipo AAAA e endereços IPv6.
- Você pode criar verificações de integridade que enviam solicitações para endereços IPv4 ou IPv6.
- Se um resolvedor de DNS estiver em uma rede IPv6, ele pode usar IPv4 ou IPv6 para enviar solicitações ao Route 53.

servidores de nome

Servidores no Domain Name System (DNS) que ajudam a converter nomes de domínio em endereços IP que os computadores usam para se comunicar entre si. Os servidores de nome podem ser recursivos (também conhecidos como DNS resolver) ou authoritative name server.

Para obter uma visão geral de como o DNS encaminha o tráfego para seus recursos, incluindo a função do Route 53 no processo, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

DNS privado

Uma versão local do Sistema de Nomes de Domínio (DNS) que permite encaminhar o tráfego de um domínio e seus subdomínios para instâncias do Amazon EC2 em uma ou mais nuvens privadas virtuais (VPCs) da Amazon. Para ter mais informações, consulte Trabalhar com zonas hospedadas privadas.

registro (registro de DNS)

Um objeto em uma zona hospedada usado para definir como você deseja rotear o tráfego para um domínio ou subdomínio. Por exemplo, você pode criar registros de exemplo.com e www.exemplo.com que roteiam o tráfego para um servidor web que tem um endereço IP 192.0.2.234.

Para obter mais informações sobre registros, incluindo informações sobre a funcionalidade fornecida pelos registros específicos do Route 53, consulte Configurar o Amazon Route 53 como serviço DNS.

servidor de nome recursivo

Consulte DNS resolver.

conjuntos de delegações reutilizáveis

Um conjunto de quatro servidores de nome autoritativos que você pode usar com mais de uma zona hospedada. Por padrão, o Route 53 atribui uma seleção aleatória de servidores de nome a cada nova zona hospedada. Para facilitar a migração do serviço de DNS de um grande número de domínios para o Route 53, você pode criar um conjunto de delegações reutilizáveis e associar esse conjunto a novas zonas hospedadas. (Você não pode alterar os servidores de nome associados a uma zona hospedada existente.)

Você cria um conjunto de delegações reutilizáveis e o associa a uma zona hospedada de forma programática. Não há suporte para o uso do console do Route 53. Para obter mais informações, consulte CreateHostedZona e CreateReusableDelegationSetna Referência da API do Amazon Route 53. O mesmo recurso também está disponível nos AWS SDKs da , na AWS Command Line Interface e no AWS Tools for Windows PowerShell.

política de roteamento

Uma configuração para registros que determina como o Route 53 responde a consultas de DNS. O Route 53 oferece suporte às seguintes políticas de roteamento:

- Simple routing policy (Política de roteamento simples): use para encaminhar o tráfego da Internet para um único recurso que executa uma determinada função para seu domínio, por exemplo, um servidor Web que fornece conteúdo para o site example.com.
- Failover routing policy (Política de roteamento de failover): use quando quiser configurar o failover ativo-passivo.
- Geolocation routing policy (Política de roteamento de localização geográfica): use quando quiser encaminhar o tráfego da Internet para seus recursos com base na localização dos usuários.
- Geoproximity routing policy (Política de roteamento de proximidade geográfica): use quando quiser encaminhar o tráfego com base no local de seus recursos e, opcionalmente, alternar o tráfego de recursos em um local para recursos em outro local.
- Latency routing policy (Política de roteamento de latência): use quando você tiver recursos em vários locais e quiser encaminhar o tráfego para o recurso que fornece a melhor latência.
- IP-based routing policy (Política de roteamento baseado em IP): use quando quiser rotear o tráfego com base no local dos usuários e tiver os endereços IP de origem do tráfego.
- Multivalue answer routing policy (Política de roteamento de resposta com vários valores): use quando quiser que o Route 53 responda a consultas de DNS com até oito registros íntegros selecionados aleatoriamente.
- Weighted routing policy (Política de roteamento ponderado): use para encaminhar o tráfego para vários recursos nas proporções que você especificar.

Para ter mais informações, consulte Escolher uma política de roteamento.

subdomínio

Um nome de domínio que tem um ou mais rótulos anexados ao nome de domínio registrado. Por exemplo, se você registrar o nome de domínio exemplo.com, www.exemplo.com é um subdomínio. Se você cria a zona hospedada contabilidade.exemplo.com do domínio exemplo.com, então seattle.contabilidade.exemplo.com é um subdomínio.

Para rotear tráfego para um subdomínio, crie um registro que tem o nome que você deseja, como www.exemplo.com, e especifique os valores aplicáveis, como o endereço IP de um servidor web.

tempo de vida (TTL)

O tempo, em segundos, pelo qual você deseja que o resolvedor de DNS armazene em cache os valores de um registro antes de enviar uma solicitação adicional ao Route 53 para obter os

valores atuais desse registro. Se o resolvedor de DNS recebe uma solicitação adicional para o mesmo domínio antes de o TTL expirar, o resolvedor retorna o valor armazenado em cache.

Um TTL mais longo reduz as cobranças do Route 53, que são parcialmente baseadas no número de consultas DNS respondidas pelo Route 53. Um TTL mais curto rediz o tempo que os resolvedores de DNS roteiam o tráfego para recursos antigos depois que você altera os valores em um registro; por exemplo, alterando o endereço IP do servidor web de www.exemplo.com.

Conceitos de planos de dados e de controle

Esta é uma visão geral dos conceitos relacionados a como o Amazon Route 53 divide sua funcionalidade em um plano de controle e um plano de dados. O serviço Route 53, como a maioria dos Serviços da AWS, inclui um plano de controle que permite executar operações de gerenciamento, como criar, atualizar e excluir recursos, e um plano de dados, que fornece a funcionalidade principal do serviço. Embora essas funcionalidades sejam desenvolvidas para serem confiáveis, os planos de controle são otimizados para consistência de dados, enquanto os planos de dados são otimizados para disponibilidade. O design resistente do plano de dados permite que ele mantenha a disponibilidade mesmo durante eventos raros de ruptura, durante os quais o plano de controle pode ficar indisponível. Por esse motivo, recomendamos o uso de funções do plano de dados em que a disponibilidade é importante.

Para verificações de saúde e DNS públicas e privadas do Route 53, o plano de controle está localizado em Região da AWS us-east-1 e os planos de dados são distribuídos globalmente.

O Amazon Route 53 está dividido em planos de dados e planos de controle, da seguinte forma:

- Para DNS público e privado do Route 53, o plano de controle é o console do Route 53 e as APIs que permitem gerenciar entradas de DNS, incluindo as APIs do Route 53 e de fluxo de tráfego. O plano de dados é o serviço DNS autoritativo, que é executado em mais de 200 locais de pontos de presença (PoP), respondendo a consultas de DNS com base nas suas zonas hospedadas e dados de verificação de integridade.
- Para verificações de integridade do Route 53, o plano de controle é o console do Route 53 e as APIs do Route 53 que você pode usar para criar, atualizar e excluir verificações de integridade. O plano de dados é o serviço globalmente distribuído, que realiza verificações de integridade, agrega os resultados e os entrega aos planos de dados do DNS público e privado do Route 53 e do AWS Global Accelerator.
- Para o Amazon Route 53 Resolver, o plano de controle consiste no console do Resolver e nas APIs que permitem gerenciar configurações da Amazon VPC, regras do Resolver, políticas de

registro em log de consultas e políticas de firewall de DNS. O plano de dados é o serviço de resolver de DNS, que responde a consultas de DNS na sua VPC, endpoints que encaminham consultas para outros resolvers e o plano de dados de Firewall de DNS que aplica políticas para filtrar consultas de DNS. O Resolver é um serviço regional e seus planos de controle e dados são executados de forma independente em cada um Região da AWS.

- Os registros de domínio do Route 53 são gerenciados somente no plano de controle na Região da AWS us-east-1.

Para obter mais informações sobre planos de dados, planos de controle e como AWS cria serviços para atingir metas de alta disponibilidade, consulte o artigo Static stability using Availability Zones na Amazon Builders' Library.

Conceitos de verificação de integridade

Aqui está uma visão geral dos conceitos relacionados à verificação de integridade do Amazon Route 53.

- DNS failover
- endpoint
- health check

failover de DNS

Um método para desviar o tráfego dos recursos com problemas de integridade e direcioná-lo para os recursos íntegros. Quando você tem mais de um recurso executando a mesma função, por exemplo, mais de um servidor Web ou um servidor de e-mail, é possível configurar as verificações de integridade do Route 53 para verificar a integridade de seus recursos e configurar registros em sua zona hospedada para encaminhar o tráfego apenas para os recursos íntegros.

Para ter mais informações, consulte Configurar failover de DNS.

endpoint

O recurso, como um servidor web ou um servidor de e-mail, para o qual você configura uma verificação de integridade. Você pode especificar um endpoint por endereço IPv4 (192.0.2.243), por endereço IPv6 (2001:0db8:85a3:0000:0000:abcd:0001:2345) ou por nome de domínio (exemplo.com).

> **Note**
>
> Você também pode criar verificações de saúde que monitorem o status de outras verificações de saúde ou que monitorem o estado do alarme de um CloudWatch alarme.

verificação de saúde

Um componente do Route 53 que permite que você faça o seguinte:

- Monitore se um endpoint especificado, como um servidor web, está íntegro;
- Opcionalmente, seja notificado quando um endpoint deixar de ser íntegro;
- Opcionalmente, configure o failover de DNS, o que permite que você redirecione o tráfego de Internet de um recurso problemático para um recurso íntegro.

Para obter mais informações sobre como criar e usar verificações de integridade, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

Como começar a usar o Amazon Route 53

Para saber mais sobre os conceitos básicos do Amazon Route 53, consulte os seguintes tópicos neste guia:

- Como configurar o Amazon Route 53, que explica como se inscrever AWS, como proteger o acesso à sua AWS conta e como configurar o acesso programático ao Route 53
- Conceitos básicos do Amazon Route 53, que descreve como registrar um nome de domínio, como criar um bucket do Amazon S3 e configurá-lo para hospedar um site estático e como encaminhar o tráfego da Internet para o site

Serviços relacionados

Para obter informações sobre os AWS serviços aos quais o Amazon Route 53 se integra, consulteIntegração com outros serviços da .

Acesso ao Amazon Route 53

Você pode acessar o Amazon Route 53 das seguintes formas:

- AWS Management Console— Os procedimentos deste guia explicam como usar o AWS Management Console para realizar tarefas.
- AWS SDKs — Se você estiver usando uma linguagem de programação que AWS fornece um SDK para, você pode usar um SDK para acessar o Route 53. Os SDKs simplificam a autenticação, integram-se com facilidade ao ambiente de desenvolvimento e fornecem acesso simples aos comandos do Route 53. Para obter mais informações, consulte Ferramentas para a Amazon Web Services.
- API do Route 53: se você estiver usando uma linguagem de programação para a qual um SDK não está disponível, consulte a Referência da API do Amazon Route 53 para obter mais informações sobre as ações de API e sobre como fazer solicitações de API.
- AWS Command Line Interface: para obter mais informações, consulte Configurar o AWS Command Line Interface no Manual do usuário do AWS Command Line Interface .
- AWS Tools for Windows PowerShell: para obter mais informações, consulte Configuração do AWS Tools for Windows PowerShell no Guia do usuário do AWS Tools for Windows PowerShell .

AWS Identity and Access Management

O Amazon Route 53 se integra ao AWS Identity and Access Management (IAM), um serviço que permite que sua organização faça o seguinte:

- Crie usuários e grupos na AWS conta da sua organização
- Compartilhe facilmente os recursos AWS da sua conta entre os usuários da conta
- Atribuir credenciais de segurança exclusivas a cada usuário
- Controlar detalhadamente o acesso do usuário a serviços e recursos

Por exemplo, você pode usar o IAM com o Route 53 para controlar quais usuários em sua AWS conta podem criar uma nova zona hospedada ou alterar registros.

Para obter mais informações sobre o IAM, consulte o seguinte:

- Gerenciamento de identidade e acesso no Amazon Route 53
- Identity and Access Management (IAM)
- Guia do usuário do IAM

Preço e cobrança do Amazon Route 53

Assim como em outros AWS produtos, não há contratos ou compromissos mínimos para usar o Amazon Route 53. Você paga somente pelas zonas hospedadas que você configurar e o número de consultas DNS respondidas pelo Route 53. Para obter mais informações, consulte Definição de preço do Amazon Route 53.

Para obter informações sobre cobrança de AWS serviços, incluindo como visualizar sua fatura e gerenciar sua conta e pagamentos, consulte o Guia do AWS Billing usuário.

Usando o Route 53 com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.

Documentação do SDK	Exemplos de código
AWS SDK for C++	AWS SDK for C++ exemplos de código
AWS CLI	AWS CLI exemplos de código
AWS SDK for Go	AWS SDK for Go exemplos de código
AWS SDK for Java	AWS SDK for Java exemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript exemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin exemplos de código
AWS SDK for .NET	AWS SDK for .NET exemplos de código
AWS SDK for PHP	AWS SDK for PHP exemplos de código
AWS Tools for PowerShell	Ferramentas para exemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemplos de código

Documentação do SDK	Exemplos de código
AWS SDK for Ruby	AWS SDK for Ruby exemplos de código
AWS SDK para Rust	AWS SDK para Rust exemplos de código
SDK da AWS para SAP ABAP	SDK da AWS para SAP ABAP exemplos de código
AWS SDK for Swift	AWS SDK for Swift exemplos de código

Para obter exemplos específicos do Route 53, consulte Exemplos de código para o Route 53 usando SDKs da AWS.

> **Exemplo de disponibilidade**
>
> Você não consegue encontrar o que precisa? Solicite um código de exemplo no link Fornecer feedback na parte inferior desta página.

Como configurar o Amazon Route 53

A visão geral e os procedimentos nesta seção ajudam você a começar com AWS.

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como uma prática recomendada de segurança, atribua o acesso administrativo para um usuário e use somente o usuário-raiz para executar tarefas que requerem o acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso para usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Fazer download das ferramentas

AWS Management Console Isso inclui um console para o Amazon Route 53, mas se você quiser acessar os serviços de forma programática, veja o seguinte:

- O guia da API documenta as operações compatíveis com os serviços e fornece links para a documentação relacionada do SDK e da CLI:
  - Referência de APIs do Amazon Route 53
- Para chamar uma API sem precisar lidar com detalhes de baixo nível, como montar solicitações HTTP brutas, você pode usar um AWS SDK. Os AWS SDKs fornecem funções e tipos de dados que encapsulam a funcionalidade dos serviços. AWS Para baixar um AWS SDK e acessar as instruções de instalação, consulte a página aplicável:
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Para obter uma lista completa dos AWS SDKs, consulte Ferramentas para Amazon Web Services.
- Você pode usar o AWS Command Line Interface (AWS CLI) para controlar vários AWS serviços na linha de comando. Você também pode automatizar seus comandos usando scripts. Para ter mais informações, consulte AWS Command Line Interface.
- AWS Tools for Windows PowerShell suporta esses AWS serviços. Para obter mais informações, consulte Referência de Cmdlets do AWS Tools for PowerShell.

Conceitos básicos do Amazon Route 53

Comece com as etapas básicas registrando um domínio com o Amazon Route 53 e configurando o Route 53 para responder a consultas de DNS que resolvem um site estático. O primeiro tutorial hospeda um site estático em um bucket aberto do Amazon S3, e o segundo tutorial usa a CloudFront distribuição da Amazon para servir o site com SSL/TLS.

Custo estimado

- Existe uma taxa anual para registrar um domínio. O valor dessa taxa varia de 9 a várias centenas de dólares e depende do domínio de nível superior, como .com. Para obter mais informações, consulte Preço do Route 53 para registro de domínio. Esta taxa não é reembolsável.
- Quando você registra um domínio, nós criamos automaticamente uma zona hospedada com o mesmo nome do domínio. Você usa a zona hospedada para especificar para onde deseja que o Route 53 encaminhe o tráfego do seu domínio.
- Durante este tutorial, você criará um bucket do Amazon S3 e carregará uma página da Web de exemplo. Se você é um novo AWS cliente, pode começar a usar o Amazon S3 gratuitamente. Se você já é um AWS cliente, as cobranças são baseadas na quantidade de dados que você armazena, no número de solicitações de seus dados e na quantidade de dados transferidos. Para obter mais informações, consulte Preços do Amazon S3.
- CloudFront as cobranças são baseadas no número de solicitações de seus dados, no número de pontos de presença que você usa e na quantidade de dados transferidos. Para obter mais informações, consulte CloudFront Preços.

Tópicos

Use seu domínio para um site estático em um bucket do Amazon S3

Este tutorial de conceitos básicos mostra como executar as seguintes tarefas:

- Registrar um nome de domínio, como exemplo.com

- Criar um bucket do Amazon S3 e configurá-lo para hospedar um site
- Criar um exemplo de site e salvar o arquivo no seu bucket do S3
- Configurar o Amazon Route 53 para encaminhar o tráfego para o seu novo site

Quando você tiver terminado, poderá abrir um navegador, digitar o nome do domínio e visualizar seu site.

> **Note**
>
> Você também pode transferir um domínio existente para o Route 53, mas o processo é mais complexo e demorado do que registrar um domínio novo. Para ter mais informações, consulte Como transferir registro de um domínio para o Amazon Route 53.

Tópicos

Pré-requisitos

Antes de começar, é necessário concluir as etapas em Como configurar o Amazon Route 53.

Etapa 1: registrar um domínio

Para usar um nome de domínio (como example.com), você deve encontrar um nome de domínio que ainda não esteja sendo usado por outra pessoa e registrá-lo. Quando você registra um nome de domínio, reserva-o para seu uso exclusivo em todos os lugares na Internet, normalmente por um ano. Por padrão, renovamos automaticamente o seu nome de domínio no final de cada ano, mas você pode desabilitar a renovação automática. Para ter mais informações, consulte Registrar um novo domínio.

Etapa 2: Criar um bucket do S3 para o domínio raiz

O Amazon S3 permite que você armazene e recupere seus dados de qualquer lugar na Internet. Para organizar os dados, você cria buckets e faz upload dos dados para os buckets usando o AWS Management Console. Você pode usar o Amazon S3 para hospedar um site estático em um bucket. O procedimento a seguir explica como criar um bucket.

Para criar um bucket do S3 para o domínio raiz

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Criar bucket.
3. Insira os seguintes valores:

   Nome do bucket

   Digite o nome do domínio, como exemplo.com.

   Região

   Escolha a região mais próxima para a maioria dos seus usuários.

   Anote a região que você escolher. Você precisará dessa informação mais adiante no processo.
4. Para aceitar as configurações padrão e criar o bucket, escolha Create bucket (Criar bucket).

Etapa 3 (opcional): Criar outro bucket do S3 para seu subdomínio

No procedimento anterior, você criou um bucket para o seu nome de domínio, como exemplo.com. Isso permite que os usuários acessem o seu site usando seu nome de domínio, como exemplo.com.

Se também quiser que os usuários usem www.*your-domain-name*, como www.example.com, para acessar seu site de exemplo, crie um segundo bucket do S3. Configure o segundo bucket para encaminhar o tráfego para o primeiro bucket.

Para criar um bucket do S3 para www.your-domain-name

1. Selecione Criar bucket.
2. Insira os seguintes valores:

   Nome do bucket

   Digite www.***your-domain-name***. Por exemplo, se você registrou o nome do domínio exemplo.com, insira www.exemplo.com.

   Região

   Escolha a mesma região na qual você criou o primeiro bucket.
3. Para aceitar as configurações padrão e criar o bucket, escolha Create (Criar).

Etapa 4: Configurar o bucket de domínio raiz para hospedagem de site

Agora que você tem um bucket do S3, você pode configurá-lo para hospedagem de site.

Para permitir a hospedagem de site em seu bucket do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista de Buckets, escolha o nome do bucket para o qual você deseja habilitar a hospedagem de site estático.
3. Escolha Properties (Propriedades).
4. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).
5. Escolha Use this bucket to host a website (Usar este bucket para hospedar um site).
6. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).
7. Em Index Document (Documento de índice), insira o nome do arquivo do documento de índice, que geralmente é `index.html`.

   O nome do documento de índice diferencia letras maiúsculas de minúsculas e deve corresponder exatamente ao nome do arquivo do documento de índice HTML do qual você planeja fazer upload para o bucket do S3. Quando você configura um bucket para hospedagem

de site, deve especificar um documento de índice. O Amazon S3 retorna esse documento de índice quando as solicitações são feitas para o domínio raiz ou alguma subpasta.

8. (Opcional) Para fornecer seu próprio documento de erro personalizado para erros de classe 4XX, em Error document (Documento de erro), insira o nome do arquivo do documento de erro personalizado.

   Se você não especificar um documento de erro personalizado e ocorrer um erro, o Amazon S3 retornará um documento de erro HTML padrão.

9. (Opcional) Se você especificar regras avançadas de redirecionamento em Redirection rules (Regras de redirecionamento), use XML para descrever as regras.

   Para saber mais, consulte o tópico sobre como Configurar redirecionamentos condicionais avançados, no Guia do usuário do Amazon Simple Storage Service.

10. Escolha Salvar alterações.
11. Em Static website hosting (Hospedagem de sites estáticos), anote o Endpoint.

    O Endpoint é o endpoint do site do Amazon S3 para o bucket. Depois de concluir a configuração do bucket como um site estático, é possível usar esse endpoint para testar o site, conforme mostrado em Etapa 9: Testar o endpoint de domínio.

    Depois de usar as seguintes etapas para editar as configurações de acesso público e adicionar uma política de bucket que permita acesso público de leitura, você pode usar o endpoint do site para acessar seu site.

Etapa 5: (opcional): Configurar o bucket de subdomínio para redirecionamento de sites

Depois de configurar o bucket do domínio raiz para hospedagem de sites, é possível configurar o bucket de subdomínios para redirecionar todas as solicitações para o domínio raiz. Por exemplo, é possível configurar todas as solicitações de `www.example.com` para serem redirecionadas para `example.com`.

Para configurar um redirecionamento

1. No console do Amazon S3, na lista de Buckets, escolha o nome do bucket do subdomínio (por exemplo, `www.example.com`).
2. Escolha Properties (Propriedades).

3. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
4. Selecione Redirect requests for an object (Redirecionar solicitações de um objeto).
5. Na caixa Target bucket (Bucket de destino), insira o domínio raiz (por exemplo, **`example.com`**).
6. Em Protocol (Protocolo), selecione http.
7. Selecione Save changes.

Etapa 6: Carregar índice para criar conteúdo do site

Ao permitir hospedagem de sites estáticos para seu bucket, você insere o nome do documento de índice (por exemplo, **`index.html`**). Depois de permitir a hospedagem de site estático para seu bucket, carregue um arquivo HTML com esse nome de documento de índice para o bucket.

Para carregar um arquivo de índice

1. Copie o seguinte exemplo de texto que você pode usar como um site simples de uma página para este tutorial, cole-o em um editor de texto e salve-o como 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. Na lista Buckets, escolha o nome do bucket para o qual você deseja habilitar a hospedagem de site estático.
3. No console do Amazon S3, escolha o nome do bucket criado no procedimento Para permitir a hospedagem de site em seu bucket do S3 (clique no nome do bucket vinculado).

4. Selecione Upload (Carregar), Add Files (Adicionar arquivos), selecione index.html de onde você o salvou e, em seguida, Upload (Carregar).
5. Se você criou um documento de erro, por exemplo, **`404.html`**, siga os passos 3 a 5 para carregá-lo.

Etapa 7: Editar configurações de bloqueio de acesso público do S3

Por padrão, o Amazon S3 bloqueia o acesso público à sua conta e aos seus buckets. Se quiser usar um bucket para hospedar um site estático, use estas etapas para editar as configurações de acesso público.

> **Warning**
>
> Antes de concluir esta etapa, revise Como bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entende e aceita os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos seus buckets.

Para rotear o tráfego para o seu site

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha o nome do bucket configurado como um site estático.
3. Escolha Permissions (Permissões).
4. Em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket), escolha Edit (Editar).
5. Desmarque Block all public access (Bloquear todo acesso público) e escolha Save changes (Salvar alterações).

O Amazon S3 desativa as configurações do Bloqueio de acesso público para seu bucket. Para criar um site público e estático, você também pode ter que editar as configurações de Bloqueio de acesso público para sua conta antes de adicionar uma política de bucket. Se as configurações da conta para bloquear acesso público estiverem ativadas no momento, você verá uma observação em Block public access (bucket settings) (Bloqueio de acesso público (configurações de bucket)).

Etapa 8: Anexar uma política de bucket

Depois de editar as configurações do Bloqueio de acesso público do Amazon S3, é possível adicionar uma política de bucket para conceder acesso público de leitura aos objetos do seu bucket. Ao conceder um acesso público de leitura, qualquer pessoa na Internet pode acessar seu bucket.

> **Warning**
>
> Antes de concluir esta etapa, revise Como bloquear o acesso público ao armazenamento do Amazon S3 para garantir que você entende e aceita os riscos envolvidos em permitir o acesso público. Ao desativar as configurações de bloqueio de acesso público para tornar seu bucket público, qualquer pessoa na Internet pode acessá-lo. Recomendamos que você bloqueie todo o acesso público aos seus buckets.

Para rotear o tráfego para o seu site

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Em Buckets, escolha o nome do seu bucket.
3. Escolha Permissions (Permissões).
4. Em Bucket Policy (Política de bucket), escolha Edit (Editar).
5. Copie a política de bucket a seguir e cole-a em um editor de texto. Esta política permite que todas as pessoas na Internet (`"Principal":"*"`) obtenham arquivos (`"Action":["s3:GetObject"]`) no bucket do S3 associado ao seu nome de domínio (`"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. Atualizar o valor de `Resource` para *`your-domain-name`*, por exemplo, **`example.com`**.
7. Escolha Salvar alterações.

Etapa 9: Testar o endpoint de domínio

Depois de configurar seu bucket de domínio para hospedar um site público, você pode testar seu endpoint. Você pode testar o endpoint somente de seu bucket de domínio porque ele está configurado para redirecionamento de site e não para hospedagem de site estático.

> **Note**
>
> O Amazon S3 não oferece suporte para o acesso HTTPS ao site. Se quiser usar HTTPS, você pode usar a Amazon CloudFront para servir um site estático hospedado no Amazon S3. Para obter mais informações, consulte Exigindo HTTPS para comunicação entre visualizadores CloudFront e.

1. Em Buckets, escolha o nome do seu bucket.
2. Escolha Properties (Propriedades).
3. Na parte inferior da página, em Static website hosting (Hospedagem estática de sites), escolha seu Bucket website endpoint (Endpoint de site do Bucket).

   Seu documento de índice é aberto em uma janela separada do navegador.

Etapa 10: Encaminhar tráfego de DNS do domínio para o bucket do site

Agora você agora tem um site de uma página no bucket do S3. Para iniciar o roteamento de tráfego de Internet do domínio para o bucket do S3, execute o procedimento a seguir.

Para rotear o tráfego para o seu site

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

> **Note**
>
> Quando você registrou seu domínio, o Amazon Route 53 criou automaticamente uma zona hospedada com o mesmo nome. Uma zona hospedada contém informações sobre como você deseja que o Route 53 encaminhe o tráfego para o domínio.

3. Na lista de zonas hospedadas, escolha o nome do domínio.
4. Escolha Create record (Criar registro).

> **Note**
>
> Cada registro contém informações sobre como você deseja encaminhar o tráfego de um domínio (como example.com) ou subdomínio (como www.example.com ou test.example.com). Os registros são armazenados na zona hospedada do domínio.

5. Escolha Switch to wizard (Alternar para assistente).
6. Escolha Simple routing (Roteamento simples) e Next (Próximo).
7. Escolha Define simple record (Definir registro simples).
8. Em Record name (Nome do registro), aceite o valor padrão, que é o nome da zona hospedada e do domínio.
9. Em Tipo de registro, escolha A - Encaminha o tráfego para um endereço IPv4 e alguns AWS recursos.
10. Em Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to S3 website endpoint (Alias para o endpoint do site do S3).
11. Escolha a região .
12. Escolha o bucket do S3.

    O nome do bucket deve corresponder ao nome que aparece na caixa Name (Nome). Na lista Choose S3 bucket (Escolher bucket do S3), o nome do bucket aparece com o endpoint do site do Amazon S3 para a região onde o bucket foi criado, por exemplo, `s3-website-us-west-1.amazonaws.com (example.com)`.

    Choose S3 bucket (Escolher o bucket do S3) lista um bucket, se uma das opções a seguir for true (verdadeira):

    - Você configurou o bucket como um site estático.

- O nome do bucket é o mesmo que o nome do registro que você está criando.
- A AWS conta atual criou o bucket.

Se o bucket não aparecer na lista Choose S3 bucket (Escolher bucket do S3), insira o endpoint de site do Amazon S3 da região em que o bucket foi criado, por exemplo, **`s3-website-us-west-2.amazonaws.com`**. Para obter uma lista completa dos endpoints do site do Amazon S3, consulte Endpoints de site do Amazon S3. Para obter mais informações sobre o destino de alias, consulte a seção “values/route traffic to” (valores/encaminhar tráfego para) em Valores específicos para registros de alias simples.

13. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
14. Escolha Define simple record (Definir registro simples).

(Opcional) Adicionar um registro de alias ao subdomínio (**`www.example.com`**)

Se você criou um bucket para seu subdomínio, adicione um registro de alias para ele também.

1. Em Configure records (Configurar registros), escolha Define simple record (Definir registro simples).
2. Em Record name (Nome do registro) para seu subdomínio, digite `www`.
3. Em Tipo de registro, escolha A - Encaminha o tráfego para um endereço IPv4 e alguns AWS recursos.
4. Em Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to S3 website endpoint (Alias para o endpoint do site do S3).
5. Escolha a região .
6. Escolha o bucket do S3, por exemplo, `s3-website-us-west-2.amazonaws.com (example.com)`.

   Se o bucket não aparecer na lista Choose S3 bucket (Escolher bucket do S3), insira o endpoint de site do Amazon S3 da região em que o bucket foi criado, por exemplo, **`s3-website-us-west-2.amazonaws.com`**.
7. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
8. Escolha Define simple record (Definir registro simples).
9. Na página Configure records (Configurar registros), escolha Create records (Criar registros).

Etapa 11: Testar o site

Para verificar se o site está funcionando corretamente, abra um navegador e pesquise os seguintes URLs:

- http://*your-domain-name* (http://seu-nome-de-domínio), por exemplo, `example.com`: exibe o documento do índice no bucket *your-domain-name*
- http://www.*your-domain-name* (por exemplo, `www.example.com`: redireciona sua solicitação para o bucket *your-domain-name*

Em alguns casos, talvez você precise limpar o cache para ver o comportamento esperado.

Para obter informações avançadas sobre o roteamento de tráfego de Internet, consulte Configurar o Amazon Route 53 como serviço DNS. Para obter informações sobre como rotear seu tráfego da Internet para AWS recursos, consulteEncaminhando o tráfego da Internet para seus recursos AWS.

Etapa 12 (opcional): use CloudFront a Amazon para acelerar a distribuição do seu conteúdo

CloudFront é um serviço da Web que acelera a distribuição de seu conteúdo estático e dinâmico da Web, como arquivos.html, .css, .js e imagens, para seus usuários. CloudFront entrega seu conteúdo por meio de uma rede mundial de data centers chamados de pontos de presença. Quando um usuário solicita conteúdo com o qual você está servindo CloudFront, ele é encaminhado para o ponto de presença que fornece a menor latência (atraso de tempo), para que o conteúdo seja entregue com o melhor desempenho possível.

- Se o conteúdo já estiver no ponto de borda com a menor latência, ele será CloudFront entregue imediatamente.
- Se o conteúdo não estiver nesse ponto de presença, CloudFront recupere-o de um bucket do Amazon S3 ou de um servidor HTTP (por exemplo, um servidor web) que você identificou como a fonte da versão definitiva do seu conteúdo.

Para obter informações sobre como usar CloudFront para distribuir o conteúdo em seu bucket do Amazon S3, consulte Adicionar CloudFront ao distribuir conteúdo do Amazon S3 no Amazon Developer Guide. CloudFront

Use uma CloudFront distribuição da Amazon para servir um site estático

Este tutorial de conceitos básicos mostra como executar as seguintes tarefas:

- Registrar um nome de domínio, como example.com.
- Criar um certificado para seu domínio.
- Criar dois buckets do Amazon S3 e configurar um para hospedar um site e o outro para redirecionar para o subdomínio.
- Criar um exemplo de site e salvar o arquivo no seu bucket do S3.
- Crie CloudFront distribuições para os dois buckets do S3.
- Configure o Amazon Route 53 para rotear o tráfego para as CloudFront distribuições.

Quando você tiver terminado, poderá abrir um navegador, inserir o nome do domínio e visualizar seu site.

Tópicos

Pré-requisitos

Antes de começar, é necessário concluir as etapas em Como configurar o Amazon Route 53.

Etapa 1: registrar um domínio

Para usar um nome de domínio (como example.com), você deve encontrar um nome de domínio que ainda não esteja sendo usado por outra pessoa e registrá-lo. Quando você registra um nome de domínio, reserva-o para seu uso exclusivo em todos os lugares na Internet, normalmente por um ano. Por padrão, renovamos automaticamente o seu nome de domínio no fim de cada ano, mas você pode desabilitar a renovação automática. Para obter mais informações, consulte Registrar um novo domínio.

Etapa 2: Solicitar um certificado público

É necessário um certificado público para que suas CloudFront distribuições da Amazon sejam configuradas CloudFront para exigir que os espectadores usem HTTPS para que as conexões sejam criptografadas quando CloudFront se comunicarem com os espectadores.

Para solicitar um certificado público AWS Certificate Manager(ACM) (console)

1. Faça login no AWS Management Console e abra o console do ACM em https://console.aws.amazon.com/acm/home.

   > **Note**
   >
   > Certifique-se de criar o certificado na região Leste dos EUA (Norte da Virgínia). Isso é necessário para a Amazon CloudFront.

   No painel de navegação esquerdo, escolha Solicitar um certificado e, na página Solicitar um certificado, escolha Solicitar um certificado público e depois Avançar.

2. Na seção Nomes de domínio, insira seu domínio, por exemplo, **`example.com`**.

   Em Adicionar outro nome para este certificado, insira um asterisco na frente do nome de domínio para solicitar um certificado curinga para todos os subdomínios, por exemplo, **`*.example.com`**.

3. Na página Método de validação, escolha Validação de DNS.
4. Na seção Algoritmo de chave, escolha RSA 2048.
5. Na seção Tags, você tem a opção de marcar seu certificado. As tags são pares de valores-chave que servem como metadados para identificar e organizar recursos. AWS

Escolha Solicitação para ser levado para a página Certificados.

6. Depois que seu novo certificado aparecer em status Pendente, escolha a ID do certificado e, na página de detalhes do certificado, escolha Criar registro no Route 53 para adicionar automaticamente os registros CNAME aos seus domínios, depois, escolha Criar registros.

   A página Certificate status (Status do certificado) deve abrir com um banner de status informando Successfully created DNS records (Registros de DNS criados com êxito).

   Seu novo certificado pode continuar a exibir um status de Validação pendente por até 30 minutos.

Etapa 3: Criar um bucket do S3 para hospedar seu subdomínio

Para criar um bucket do S3 para www.your-domain-name

O Amazon S3 permite que você armazene e recupere seus dados de qualquer lugar na Internet. Nesta etapa, você cria um bucket do S3 para armazenar todos os arquivos do seu site.

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Criar bucket.
3. Insira os seguintes valores:

   Nome do bucket

   Digite www.***your-domain-name***. Por exemplo, se você registrou o nome do domínio exemplo.com, insira www.exemplo.com.

   Região

   Escolha uma região para seu bucket.
4. Para aceitar as configurações padrão e criar o bucket, escolha Create bucket (Criar bucket).

   Para obter mais informações sobre as configurações de bucket do S3, consulte View bucket properties (Visualizar propriedades de buckets) no Manual do usuário do Amazon S3.

Etapa 4: Criar outro bucket do S3 para seu domínio raiz

Se você também quiser que seus usuários usem o domínio raiz, *.your-domain-name* (como example.com) para acessar seu site de exemplo, crie um segundo bucket do S3. Neste tutorial, você vai configurar o segundo bucket (domínio raiz) para rotear o tráfego para o primeiro bucket.

Para criar um bucket do S3 para your-domain-name

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Criar bucket.
3. Insira os seguintes valores:

   Nome do bucket

   Digite ***your-domain-name***. Por exemplo, se você registrou o nome do domínio example.com, insira example.com.

   Região

   Escolha a mesma região na qual você criou o primeiro bucket.
4. Para aceitar as configurações padrão e criar o bucket, escolha Create bucket (Criar bucket).

Etapa 5: Carregar arquivos de site para seu bucket de subdomínio

Agora que você tem um bucket do S3, você pode carregar os arquivos do site. Neste tutorial você vai apenas carregar um arquivo simples index.html que exibe uma página de texto.

Habilitar seu bucket do S3 para hospedagem de site

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista de Buckets, escolha o nome vinculado do bucket no qual você deseja carregar os arquivos do site, como **www.example.com**.
3. Copie o texto de exemplo que cria um site simples de uma página, cole-o em um editor de texto e salve-o como 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. Na guia Objects (Objetos), escolha Upload (Carregar).
5. Em Files and folders (Arquivos e pastas), escolha Add files (Adicionar arquivos) e carregue os arquivos do seu site. Para este tutorial, faça upload do arquivo index.html que você salvou na etapa 3 deste procedimento.

Etapa 6: Configurar o bucket de domínio raiz para redirecionamento de sites

Depois de configurar o bucket do domínio raiz para hospedagem de sites, você tem a opção de configurar o bucket do domínio raiz para redirecionar todas as solicitações para o subdomínio. Por exemplo, é possível configurar todas as solicitações de `example.com` para serem redirecionadas para `www.example.com`.

Para configurar um redirecionamento

1. No console do Amazon S3, na lista de Buckets, escolha o nome do bucket (por exemplo, `example.com`).
2. Escolha Properties (Propriedades).
3. Em Static website hosting (Hospedagem estática de sites), escolha Edit (Editar).
4. Em Static website hosting (Hospedagem estática de sites), escolha Enable (Ativar).
5. Selecione Redirect requests for an object (Redirecionar solicitações de um objeto).
6. Na caixa Host name (Nome do host), insira seu subdomínio, por exemplo, **`www.example.com`**.
7. Em Protocol, escolha HTTPS.

8. Escolha Salvar alterações.
9. Em Static website hosting (Hospedagem de sites estáticos), anote o Endpoint.

   O Endpoint é o endpoint do site do Amazon S3 para o bucket. Você usará esse endpoint para configurar uma CloudFront distribuição da Amazon.

Etapa 7: Crie uma CloudFront distribuição da Amazon para seu subdomínio

Nesta etapa, você cria uma CloudFront distribuição para seu subdomínio, como www.exemplo.com, para permitir que seu site use HTTPS para que as pessoas possam visualizá-lo com segurança.

Para criar uma distribuição do CloudFront

1. Abra o CloudFront console emhttps://console.aws.amazon.com/cloudfront/v4/home.
2. Escolha Criar distribuição.
3. Em Origem, para Nome de domínio de origem, escolha o bucket do Amazon S3 que você criou anteriormente. O formato será semelhante **`www.example.com.s3.<Region>.amazonaws.com`** a.

   Para Acesso de origem, selecione Identidades de acesso legadas. Para Origin access identity (Identidade do acesso de origem), você pode escolher na lista ou escolher Create new OAI (Criar novo OAI) (ambos funcionarão).

   Para Bucket policy (Política de bucket), selecione Yes, update the bucket policy (Sim, atualizar a política de bucket).
4. Para as configurações em Default Cache Behavior Settings (Configurações de comportamento de cache padrão), em Viewer (Visualizador), defina Viewer protocol policy (Política de protocolo Visualizador) como Redirect HTTP to HTTPS (Redirecionar HTTP para HTTPS) e aceite os valores padrão para os outros.

   Para obter mais informações sobre as opções de comportamento do cache, consulte Configurações de comportamento do cache no guia do CloudFront desenvolvedor da Amazon.
5. Na seção Web Application Firewall (WAF), você pode optar por habilitar ou desabilitar as proteções de segurança AWS WAF .
6. Para os campos, em Settings (Configurações), faça o seguinte:

- Selecione Add item (Adicionar item) para Alternate domain name (CNAME) - optional (Nome de domínio alternativo (CNAME) - opcional e insira seu subdomínio, como **`www.example.com`**.
- Para Custom SSL Certificate (Certificado SSL personalizado), selecione o certificado que você criou anteriormente.
- Na caixa de texto Default root object Objeto raiz padrão, digite **`index.html`**.
- Aceite os valores padrão dos demais campos e escolha Criar distribuição.

  Para obter mais informações sobre opções de distribuição, consulte Distribution settings (Configurações de distribuição).

7. Depois de CloudFront criar sua distribuição, o valor da coluna Status da sua distribuição muda de Em andamento para Implantado. Normalmente, isso demora alguns minutos.

   Registre o nome de domínio CloudFront atribuído à sua distribuição, que aparece na lista de distribuições. Você pode usar esse nome de domínio para testar a distribuição.

Etapa 8: Crie uma CloudFront distribuição da Amazon para seu domínio raiz

Nesta etapa, você cria uma CloudFront distribuição para seu domínio raiz para que ele use HTTPS quando o URL for redirecionado para o subdomínio.

Para criar uma distribuição do CloudFront

1. Abra o CloudFront console emhttps://console.aws.amazon.com/cloudfront/v4/home.
2. Escolha Criar distribuição.
3. Em Origin Settings (Configurações de Origem), para Origin Domain Name (Nome do Domínio de Origem), insira o endpoint do site do bucket. Você obtém isso na seção Static website hosting (Hospedagem de site estático) de Properties (Propriedades) para o bucket do Amazon S3 que você criou anteriormente.

   Para o restante, aceite os valores padrão.
4. Na seção Web Application Firewall (WAF), você pode optar por habilitar ou desabilitar as proteções de segurança AWS WAF .

5. Para os campos em Chave de cache e solicitações de origem, escolha Política de cache e Política de solicitações de origem (recomendado) e, no menu suspenso Política de cache, escolha CachingDisabled

   Para o restante, aceite os valores padrão.

   Para obter mais informações sobre as opções de comportamento do cache, consulte Configurações de comportamento do cache no guia do CloudFront desenvolvedor da Amazon.
6. Para os campos, em Settings (Configurações), faça o seguinte:

   - Escolha Add item (Adicionar item) para Alternate domain name (CNAME) - optional (Nome de domínio alternativo (CNAME) - opcional) e insira seu domínio raiz, como **`example.com`**.
   - Para Custom SSL Certificate (Certificado SSL personalizado), selecione o certificado que você criou anteriormente.
   - Para o restante, aceite os valores padrão.

   Para obter mais informações sobre opções de distribuição, consulte Distribution settings (Configurações de distribuição).
7. Na parte inferior da página, escolha Create Distribution (Criar distribuição).
8. Depois de CloudFront criar sua distribuição, o valor da coluna Status da sua distribuição muda de Em andamento para Implantado. Normalmente, isso demora alguns minutos.

   Registre o nome de domínio CloudFront atribuído à sua distribuição, que aparece na lista de distribuições. Você pode usar esse nome de domínio para testar a distribuição,

Etapa 9: rotear o tráfego DNS do seu domínio para sua distribuição CloudFront

Agora você tem um site de uma página em seu bucket do S3 que usa uma CloudFront distribuição. Para começar a rotear o tráfego da Internet do seu domínio para a CloudFront distribuição, execute o procedimento a seguir.

Para obter mais informações sobre o roteamento do tráfego para CloudFront distribuições, consulte. Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio

Para rotear o tráfego para o seu site

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

   > **Note**
   >
   > Quando você registrou seu domínio, o Amazon Route 53 criou automaticamente uma zona hospedada com o mesmo nome. Uma zona hospedada contém informações sobre como você deseja que o Route 53 encaminhe o tráfego para o domínio.

3. Na lista de zonas hospedadas, escolha o nome do domínio.
4. Escolha Create record (Criar registro).

   Se você estiver na exibição Quick create record (Criação rápida de registro), escolha Switch to wizard (Alternar para assistente).

   > **Note**
   >
   > Cada registro contém informações sobre como você deseja rotear o tráfego de um domínio (como exemplo.com) ou subdomínio (como www.exemplo.com ou teste.exemplo.com). Os registros são armazenados na zona hospedada do domínio.

5. Escolha Simple routing (Roteamento simples) e Next (Próximo).
6. Escolha Define simple record (Definir registro simples).
7. Em Record name (Nome do registro), digite **www** na frente do valor padrão, que é o nome da zona hospedada e do domínio.
8. Em Tipo de registro, escolha A - Encaminha o tráfego para um endereço IPv4 e alguns AWS recursos.
9. Em Valor/Rotear tráfego para, escolha Alias para distribuição. CloudFront
10. Escolha a distribuição.

    O nome da distribuição deve corresponder ao nome que aparece na caixa Domain name (Nome de domínio) na lista Distributions(Distribuições), por exemplo, `dddjjjkkk.cloudfront.net`.
11. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
12. Escolha Define simple record (Definir registro simples).

Como adicionar um registro de alias ao domínio raiz (**`example.com`**)

Adicionar um registro de alias para seu domínio raiz também, de modo que ele aponte para o bucket do S3 que redireciona o tráfego para `www.example.com`. Para obter mais informações sobre o roteamento do tráfego para CloudFront distribuições, consulte. Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio

1. No painel de navegação, escolha Zonas hospedadas.
2. Na lista de zonas hospedadas, escolha o nome do domínio.
3. Escolha Create record (Criar registro).

   Se você estiver na exibição Quick create record (Criação rápida de registro), escolha Switch to wizard (Alternar para assistente).

   > **Note**
   >
   > Cada registro contém informações sobre como você deseja rotear o tráfego de um domínio (como exemplo.com) ou subdomínio (como www.exemplo.com ou teste.exemplo.com). Os registros são armazenados na zona hospedada do domínio.

4. Escolha Simple routing (Roteamento simples) e Next (Próximo).
5. Escolha Define simple record (Definir registro simples).
6. Em Record name (Nome de registro), aceite o valor padrão.
7. Em Tipo de registro, escolha A - Encaminha o tráfego para um endereço IPv4 e alguns AWS recursos.
8. Em Valor/Rotear tráfego para, escolha Alias para distribuição. CloudFront
9. Escolha a distribuição.

   O nome da distribuição deve corresponder ao nome que aparece na caixa Domain name (Nome de domínio) na lista Distributions(Distribuições), por exemplo, `dddjjjkkk.cloudfront.net`.
10. Em Evaluate target health (Avaliar integridade do destino), escolha No (Não).
11. Escolha Define simple record (Definir registro simples).
12. Na página Configure records (Configurar registros), escolha Create records (Criar registros).

Etapa 10: Testar o site

Para verificar se o site está funcionando corretamente, abra um navegador e pesquise os seguintes URLs:

- https://www.*your-domain-name*, por exemplo, `www.example.com`: exibe o documento de índice no bucket *www.your-domain-name*
- http://www.*your-domain-name*, por exemplo, `example.com`: redireciona sua solicitação para o bucket *your-domain-name*

Em alguns casos, talvez você precise limpar o cache para ver o comportamento esperado.

Para obter informações avançadas sobre o roteamento de tráfego de Internet, consulte Configurar o Amazon Route 53 como serviço DNS. Para obter informações sobre como rotear seu tráfego da Internet para AWS recursos, consulteEncaminhando o tráfego da Internet para seus recursos AWS.

Integração com outros serviços da

Você pode integrar o Amazon Route 53 a outros serviços da AWS para registrar as solicitações enviadas à API do Route 53, monitorar o status de seus recursos e atribuir tags aos seus recursos. Além disso, você pode usar o Route 53 para encaminhar o tráfego de Internet para seus recursos da AWS.

Tópicos

Registrar, monitorar e marcar

AWS CloudTrail

O Amazon Route 53 é integrado ao AWS CloudTrail, um serviço que captura informações sobre cada solicitação enviada à API do Route 53 pela sua conta da AWS. Você pode usar as informações dos arquivos de log do CloudTrail para determinar quais solicitações foram feitas ao Route 53, o endereço IP de origem do qual cada solicitação foi feita, quem a fez, quando ela foi feita e assim por diante.

Para obter mais informações, consulte Registro de chamadas de API do Amazon Route 53 com AWS CloudTrail.

Amazon CloudWatch

Você pode usar o Amazon CloudWatch para monitorar o status, íntegro ou não íntegro, de suas verificações de integridade do Route 53. Essas verificações monitoram a integridade e a performance de suas aplicações Web, servidores Web e outros recursos. Em intervalos regulares que você especifica, o Route 53 envia solicitações automatizadas pela Internet para sua aplicação, servidor ou outro recurso, a fim de verificar se está acessível, disponível e funcional.

Para obter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

Tag Editor

Uma tag é um rótulo atribuído a um recurso da AWS, incluindo domínios do Route 53, zonas hospedadas e verificações de integridade. Cada tag consiste em uma chave e um valor, ambos definidos por você. Por exemplo, você pode atribuir uma tag a um registro de domínio que tenha a chave “Customer” (Cliente) e o valor “Examplo Corp” (Exemplo Corp). Você pode usar tags para uma variedade de propósitos; um uso comum é a categorização e o rastreamento dos custos do AWS.

Para obter mais informações, consulte Marcação de recursos do Amazon Route 53.

Encaminhar tráfego para outros recursos da AWS

Você pode usar o Amazon Route 53 para encaminhar o tráfego para uma variedade de recursos da AWS.

Amazon API Gateway

O Amazon API Gateway permite que você crie, publique, mantenha, monitore e proteja APIs em qualquer escala. Você pode criar APIs que acessam a AWS ou outros serviços Web, bem como dados armazenados na Nuvem AWS.

Você pode usar o Route 53 para encaminhar o tráfego para uma API do API Gateway. Para obter mais informações, consulte Encaminhar o tráfego para uma API do Amazon API Gateway por meio do seu nome de domínio.

Amazon CloudFront

Para acelerar a entrega do seu conteúdo da Web, você pode usar o Amazon CloudFront, a rede de entrega de conteúdo (CDN) da AWS. O CloudFront pode ser usado para distribuir todo o seu site, (incluindo conteúdos dinâmicos, estáticos, transmissão e conteúdo interativo) utilizando uma rede internacional de locais da borda. O CloudFront encaminha solicitações do seu conteúdo para o local da borda que oferece aos usuários a mais baixa latência. Você pode usar o Route 53 para encaminhar o tráfego do seu domínio para a sua distribuição do CloudFront. Para obter mais informações, consulte Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio.

Amazon EC2

O Amazon EC2 fornece capacidade computacional escalável na Nuvem AWS. Você pode iniciar um ambiente de computação virtual EC2 (uma instância) usando um modelo pré-configurado

(uma Imagem de máquina da Amazon ou AMI). Quando você inicia uma instância do EC2, o EC2 instala automaticamente o sistema operacional (Linux ou Microsoft Windows) e o software adicional incluído no AMI, tal como o servidor web ou o software de banco de dados.

Se você hospedar um site ou executar uma aplicação Web em uma instância do EC2, poderá encaminhar o tráfego do seu domínio, como exemplo.com, para o seu servidor usando o Route 53. Para obter mais informações, consulte Como encaminhar o tráfego para uma instância do Amazon EC2.

AWS Elastic Beanstalk

Se você usar o AWS Elastic Beanstalk para implantar e gerenciar aplicações na Nuvem AWS, pode usar o Route 53 para encaminhar o tráfego DNS de seu domínio, como example.com, para um ambiente do Elastic Beanstalk. Para obter mais informações, consulte Roteamento do tráfego para um ambiente AWS Elastic Beanstalk.

Elastic Load Balancing

Se hospedar um site em várias instâncias do Amazon EC2, você poderá distribuir o tráfego para seu site através das instâncias usando um balanceador de carga do Elastic Load Balancing (ELB). O serviço do ELB escala automaticamente o load balancer conforme o tráfego para o seu site sofre mudanças. O load balancer também pode monitorar a integridade das suas instâncias registradas e rotear somente o tráfego de domínio para instâncias íntegras.

Você pode usar o Route 53 para encaminhar o tráfego de seu domínio para o Classic, a aplicação ou o Network Load Balancer. Para obter mais informações, consulte Rotear tráfego para um load balancer do ELB.

Amazon Lightsail

O Amazon Lightsail fornece capacidade de computação, de armazenamento e de redes, além de recursos para implantar e gerenciar sites, aplicações Web e bancos de dados na nuvem por um preço mensal baixo e previsível.

Se você usar o Lightsail, é possível usar o Route 53 para encaminhar o tráfego para sua instância do Lightsail. Para obter mais informações, consulte Como usar o Route 53 para apontar um domínio para uma instância do Amazon Lightsail.

Amazon S3

O Amazon Simple Storage Service (Amazon S3) oferece um armazenamento na nuvem altamente escalável, seguro e duradouro. Você pode configurar um bucket do S3 para hospedar

um site estático que pode incluir páginas da web e scripts do lado do cliente. (O S3 não oferece suporte para script de servidor.) Você pode usar o Route 53 para encaminhar o tráfego para um bucket do Amazon S3. Para obter mais informações, consulte os tópicos a seguir:

- Para obter informações sobre o roteamento de tráfego para um bucket, consulte Como encaminhar o tráfego para um site hospedado em um bucket do Amazon S3.
- Para obter uma explicação mais detalhada sobre como hospedar um site estático em um bucket do S3, consulte Conceitos básicos do Amazon Route 53.

Amazon Virtual Private Cloud (Amazon VPC)

Um endpoint de interface permite que você se conecte a serviços desenvolvidos pelo AWS PrivateLink. Esses serviços incluem alguns serviços da AWS, serviços hospedados por outros clientes e parceiros da AWS em suas próprias VPCs (chamados de serviços de endpoint) e serviços compatíveis de parceiros do AWS Marketplace.

Você pode usar o Route 53 para encaminhar o tráfego para um endpoint de interface. Para obter mais informações, consulte Como encaminhar o tráfego para um endpoint de interface da Amazon Virtual Private Cloud por meio do seu nome de domínio.

Amazon WorkMail

Se estiver usando o Amazon WorkMail para o seu e-mail comercial e o Route 53 como seu serviço DNS, você poderá encaminhar o tráfego para o seu domínio de e-mail do Amazon WorkMail por meio do Route 53. Para obter mais informações, consulte Roteamento de tráfego para a Amazon WorkMail.

Para mais informações, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Formato de nome de domínio DNS

Os nomes de domínio (incluindo os nomes de domínios, zonas hospedadas e registros) consistem em uma série de rótulos separados por pontos. Um rótulo pode ter até 63 bytes de tamanho. O tamanho total de um nome de domínio não pode exceder 255 bytes, incluindo os pontos. O Amazon Route 53 oferece suporte a qualquer nome de domínio válido.

Os requisitos de nomenclatura dependem de você estar registrando um nome de domínio ou estar especificando o nome de uma zona hospedada ou de um registro. Consulte o tópico aplicável.

Tópicos

Formatar nomes de domínio para registro de nome de domínio

Para o registro de nome de domínio, um nome de domínio pode conter apenas os caracteres a-z, 0-9 e - (hífen). Você não pode especificar um hífen no início ou no fim de um rótulo.

Para obter informações sobre como registrar um Internationalized Domain Name (IDN – Nome de domínio internacionalizado), consulte Formatar nomes de domínio internacionalizados.

Formatar nomes de domínio para zonas hospedadas e registros

Para zonas hospedadas e registros, o nome de domínio pode incluir qualquer um dos seguintes caracteres ASCII imprimíveis (exceto espaços):

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

O Amazon Route 53 armazena caracteres alfabéticos como letras minúsculas (a-z), independentemente de como você as especifica: como letras maiúsculas, minúsculas ou letras em códigos de escape correspondentes.

Se o seu nome de domínio contiver os caracteres a seguir, você deve especificar os caracteres usando códigos de escape no formato *código octal de três dígitos*:

- Os caracteres 000 a 040 octal (0 a 32 decimal, 0x00 a 0x20 hexadecimal)
- Os caracteres 177 a 377 octal (127 a 255 decimal, 0x7F a 0xFF hexadecimal)
- . (ponto), caractere 056 octal (46 decimal, 0x2E hexadecimal), quando usados como um caractere em um nome de domínio. Ao usar o . (ponto) como um delimitador entre rótulos, você não precisa usar um código de escape.

Se o nome de domínio incluir quaisquer caracteres que não sejam de a a z, de 0 a 9, um hífen (–) ou um sublinhado (_), as ações da API do Route 53 retornam os caracteres como códigos de escape. Isso é verdadeiro se você especificar os caracteres como caracteres ou códigos de escape quando criar a entidade. O console do Route 53 exibe os caracteres como caracteres, não como códigos de escape.

Para obter uma lista de caracteres ASCII e os códigos octais correspondentes, pesquise o termo “tabela ascii” na Internet.

Para especificar um Internationalized Domain Name (IDN – Nome de domínio internacionalizado), converta o nome para Punycode. Para obter mais informações, consulte Formatar nomes de domínio internacionalizados.

Usar um asterisco (*) nos nomes de zonas hospedadas e registros

É possível criar zonas hospedadas e registros que incluam * no nome.

Zonas hospedadas

- Você não pode incluir um * no rótulo mais à esquerda em um nome de domínio. Por exemplo, não é permitido usar *.exemplo.com.
- Se você incluir o * em outras posições, o DNS o tratará como um caractere * (ASCII 42), e não como um curinga.

Registros

O DNS trata o caractere * como um caractere curinga ou como o caractere * (ASCII 42), dependendo de onde ele aparece no nome. Observe as seguintes restrições sobre o uso do * como caractere curinga no nome de um registro:

- O * deve substituir o rótulo mais à esquerda em um nome de domínio, por exemplo, *.exemplo.com ou *.acme.exemplo.com. Se você incluir o * em outras posições, como prod.*.exemplo.com, o DNS o tratará como um caractere * (ASCII 42), e não como um curinga.
- O * deve substituir todo o rótulo. Por exemplo, você não pode especificar *prod.exemplo.com ou prod*.exemplo.com.
- Nomes específicos de domínio têm precedência. Por exemplo, se você criar registros para *.exemplo.com e acme.exemplo.com, o Route 53 sempre responderá às consultas DNS para acme.exemplo.com com os valores do registro acme.exemplo.com.
- O * se aplica a consultas de DNS para o nível de subdomínio que inclui o asterisco e todos os subdomínios desse subdomínio. Por exemplo, se você criar um registro chamado *.exemplo.com, o Route 53 usará os valores desse registro para responder a consultas DNS para zenith.exemplo.com, acme.zenith.exemplo.com e pinnacle.acme.zenith.exemplo.com (se não houver registros de qualquer tipo para essa zona hospedada).

  Se você criar um registro chamado *.exemplo.com e não houver nenhum registro exemplo.com, o Route 53 responderá às consultas DNS para exemplo.com com `NXDOMAIN` (domínio inexistente).
- É possível configurar o Route 53 para retornar a mesma resposta a consultas DNS tanto para todos os subdomínios do mesmo nível como para o nome de domínio. Por exemplo, você pode configurar o Route 53 para responder a consultas DNS como acme.exemplo.com e zenith.exemplo.com usando o registro exemplo.com. Siga estas etapas:

  1. Crie um registro do domínio, como example.com.
  2. Crie um registro de alias para o subdomínio, como *.example.com. Especifique o registro criado na etapa 1 como o destino do registro de alias.
- Você não pode usar o * como um curinga para registros que tenham um tipo NS.

Formatar nomes de domínio internacionalizados

Ao registrar um novo nome de domínio ou criar zonas hospedadas e registros, você pode especificar letras diferentes de a-z (por exemplo, o ç em França), caracteres em outros alfabetos (por exemplo, cirílico ou árabe) e caracteres em chinês, japonês ou coreano. O Amazon Route 53 armazena esses

nomes de domínio internacionalizados (IDNs) em Punycode, que representa caracteres Unicode como strings ASCII.

Se você estiver registrando um nome de domínio, observe o seguinte:

- Só é possível usar caracteres diferentes de a-z, 0-9 e - (hífen) se o Top-Level Domain (TLD – Domínio de nível superior) oferecer suporte a IDNs e ao idioma que você pretende usar. Para determinar com quais idiomas um TLD é compatível, consulte Domínios que você pode registrar com o Amazon Route 53.
- É possível especificar um nome em um idioma não compatível se o nome contiver apenas as letras a-z. Por exemplo, se um TLD não oferecer suporte ao francês, mas o nome que você deseja usar incluir apenas os caracteres a-z sem marcas diacríticas, ainda será possível usar esse nome. Neste exemplo, um nome que inclui um “c” é permitido; um nome que contém um “ç” não é.
- Se um TLD não oferecer suporte a IDNs ou ao idioma que você pretende usar no nome de domínio, também não será possível especificar o nome em Punycode, mesmo que o Punycode inclua apenas a-z, 0-9 e -.

O exemplo a seguir mostra a representação Punycode do nome de domínio internacionalizado 中国.asia:

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

Quando você digita um IDN na barra de endereços de um navegador moderno, o navegador converte esse nome em Punycode antes de enviar uma consulta de DNS ou fazer uma solicitação HTTP.

A forma como você insere um IDN depende do que você está criando (nomes de domínio, zonas hospedadas ou registros) e de como está criando (API, SDK ou console do Route 53):

- Se você estiver usando a API do Route 53 ou um dos SDKs da AWS, pode converter um valor Unicode em Punycode de forma programática. Por exemplo, se você estiver usando o Java, pode converter um valor Unicode em Punycode usando o método toASCII da biblioteca java.net.IDN.
- Se você estiver usando o console do Route 53 para registrar um nome de domínio, pode colar o nome, incluindo caracteres Unicode, no campo de nome e o console converterá o valor em Punycode antes de salvá-lo.
- Se estiver usando o console do Route 53 para criar zonas hospedadas ou registros, você precisará converter o nome de domínio em Punycode antes de inserir o nome no campo Name

(Nome) aplicável. Para obter informações sobre conversores online, pesquise “conversor punycode” na Internet.

Se você estiver registrando um nome de domínio, observe que nem todos os Top-Level Domains (TLD – Domínio de nível superior) oferecem suporte a IDNs. Para ver uma lista dos TLDs compatíveis com o Route 53, consulte Domínios que você pode registrar com o Amazon Route 53. Os TLDs que não oferecem suporte a IDNs estão indicados.

Registrar e gerenciar novos domínios com o Amazon Route 53

Quando você deseja obter um novo nome de domínio, como a parte example.com do URL http://example.com, pode registrá-lo no Amazon Route 53. Você também pode transferir o registro de domínios existentes de outros registradores para o Route 53 ou transferir o registro de domínios registrados no Route 53 para outro registrador.

Os procedimentos neste capítulo explicam como registrar e transferir os domínios usando o console do Route 53 e como editar as configurações e visualizar o status do domínio. Se você está apenas registrando e gerenciando alguns domínios, a maneira mais fácil de fazer isso é com o console.

Se você precisa registrar e gerenciar muitos domínios, convém fazer alterações de maneira programática. Para ter mais informações, consulte Como configurar o Amazon Route 53.

> **Note**
>
> Se você estiver usando uma linguagem para a qual existe um AWS SDK, use o SDK em vez de tentar trabalhar com as APIs. Os SDKs simplificam a autenticação, integram-se facilmente ao ambiente de desenvolvimento e fornecem acesso fácil aos comandos do Route 53.

Os serviços de registro de nomes de domínio são fornecidos de acordo com nosso Acordo de registro de nomes de domínio.

Tópicos

- Como encontrar seu registrador e outras informações sobre seu domínio
- Excluir um registro de nome de domínio
- Entrar em contato com o AWS Support sobre problemas de registro de domínio
- Fazer download de um relatório de faturamento de domínios
- Domínios que você pode registrar com o Amazon Route 53

Registrar novos domínios

Para obter informações sobre o registro de novos domínios, a transferência de um domínio e a visualização do status do registro do domínio, consulte o tópico aplicável.

Tópicos

- Registrar um novo domínio
- Valores que você especifica ao registrar ou transferir um domínio
- Valores que o Amazon Route 53 retorna quando você registra um domínio
- Visualizar o status do registro de um domínio

Registrar um novo domínio

Registrar um novo domínio ou atualizar os servidores de nomes de um domínio existente

Você pode usar o Amazon Route 53 com domínios que você registra com o Route 53, e com domínios que você registrou com outros provedores de DNS. Dependendo do seu provedor DNS, escolha um dos seguintes procedimentos para registrar e usar um novo domínio com o Route 53:

- Para registrar um novo domínio, consulte Para registrar um novo domínio usando o Route 53.
- Para um domínio existente, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.
- Para passar um domínio para outro registrador, consulte update name servers when you want to use another DNS service.

Considerações sobre registro de domínio

Antes de começar, verifique o seguinte:

Entrando em contato com AWS o Suporte

Se você tiver problemas ao registrar um domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Definição de preço do registro de domínio

Para obter informações sobre o custo para registrar domínios, consulte Preço do Amazon Route 53 para registro de domínio.

Domínios compatíveis

Para ver uma lista dos TLDs, consulte Domínios que você pode registrar com o Amazon Route 53.

Você não pode alterar um nome de domínio depois de registrá-lo

Se você acidentalmente registrar o nome de domínio errado, não poderá alterá-lo. Em vez disso, você precisa registrar outro nome de domínio e especificar o nome correto. Você também não pode receber um reembolso para um nome de domínio que registrou acidentalmente.

AWS créditos

Você não pode usar AWS créditos para pagar a taxa de registro de um novo domínio no Route 53.

Preços especiais ou premium

Os registros de TLD atribuíram preços especiais ou premium a alguns nomes de domínio. Não é possível usar o Route 53 para registrar um domínio que tenha um preço especial ou premium.

Mudanças para zonas hospedadas

Quando você registra um domínio com o Route 53, nós criamos automaticamente uma zona hospedada para ele e cobramos uma pequena taxa mensal por essa zona, além da taxa anual pelo registro do domínio. Essa zona hospedada é onde você armazena informações sobre como rotear o tráfego do seu domínio, por exemplo, para uma instância do Amazon EC2 ou uma CloudFront distribuição. Se você não deseja usar seu domínio agora, pode excluir a zona hospedada. Se você a excluir até 12 horas após o registro do domínio, não haverá nenhuma cobrança pela zona hospedada na fatura da AWS . Também cobramos uma pequena taxa para as consultas de DNS que recebemos para o seu domínio. Para obter mais informações, consulte Definição de preço do Amazon Route 53.

Substituir a zona hospedada de um domínio

Se você criar uma nova zona hospedada para um domínio, deverá também atualizar os servidores de nomes de domínio para usar os mesmos servidores de nomes que a nova zona hospedada. Para obter mais detalhes, consulte Como substituir a zona hospedada por um domínio registrado com o Route 53

Para registrar um novo domínio usando o Route 53

Para registrar um novo domínio usando o Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios e depois Domínios registrados.
3. Na página Domínios registrados, escolha Registrar domínios.

   a. Na seção Pesquisar domínio, insira o nome de domínio que você deseja registrar e escolha Pesquisar para descobrir se o nome do domínio está disponível.

      Se o nome de domínio que você deseja registrar contiver caracteres diferentes de a-z, A-Z, 0-9 e - (hífen), observe o seguinte:

      - Você pode inserir o nome usando os caracteres aplicáveis. Você não precisa converter o nome em Punycode.
      - Uma lista de idiomas é exibida. Escolha o idioma do nome especificado. Por exemplo, se você digitar příklad (“exemplo” em checo), escolha Checo (CES) ou Checo (CZE).

      > **Note**
      >
      > Para idiomas que têm mais de um código, talvez seja necessário tentar ambos. Embora CES e CZE sejam sinônimos, alguns registros TLD são compatíveis apenas com um ou outro.

      Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Se o domínio que você inseriu estiver disponível, ele será exibido; caso contrário, domínios semelhantes serão exibidos como sugestões.

Você pode escolher até cinco domínios para registrar. Os domínios selecionados aparecem na lista Domínios selecionados.

b. Para registrar mais domínios, repita as etapas de 3a a 3b.

4. Escolha Prosseguir para finalizar a compra.
5. Na página Preços, escolha por quantos anos você deseja registrar o domínio e se deseja que renovemos automaticamente o registro do domínio antes da data de expiração.

> **Note**
>
> Os registros e as renovações de nome de domínio não são restituíveis. Se você habilitar a renovação automática do domínio e decidir que não deseja o nome de domínio depois de renovar o registro, não poderá receber reembolso para o custo da renovação.

Selecione Next (Próximo).

6. Na página Informações de contato, insira as informações de contato do registrante do domínio, do administrador, do técnico e dos contatos de cobrança. Os valores informados aqui são aplicados a todos os domínios que você está registrando. Para ter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

Observe as seguintes considerações:

Nome e sobrenome

Para First Name e Last Name, recomendamos que você especifique o nome no seu ID oficial. Para determinadas mudanças nas configurações do domínio, alguns registros de domínio exigem que você forneça prova de identidade. O nome no documento de identificação precisa corresponder ao nome no contato do registrante para o domínio.

Contatos diferentes

Por padrão, usamos as mesmas informações para os três contatos. Se quiser inserir informações diferentes para um ou mais contatos, desmarque a caixa ao lado de Igual ao do registrante.

> **Note**
>
> Para os domínios .it, o registrante e os contatos administrativos devem ser os mesmos.

> **Note**
>
> Para domínios.jp, os contatos técnicos e administrativos devem ser os mesmos.

Vários domínios

Se você registrar mais de um domínio, usaremos as mesmas informações de contato para todos os domínios.

Informações necessárias adicionais

Para alguns domínios de nível superior (TLDs), é necessário coletar informações adicionais. Para esses TLDs, insira os valores aplicáveis depois do campo CEP.

Proteção da privacidade

Escolha se você deseja ocultar suas informações de contato de consultas WHOIS.

> **Note**
>
> Você deve especificar a mesma configuração de privacidade para os contatos administrativos, registrantes, técnicos e de cobrança.

Para obter mais informações, consulte os tópicos a seguir.

- Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio
- Domínios que você pode registrar com o Amazon Route 53

> **Note**
>
> Para habilitar a proteção de privacidade para os domínios .uk, .co.uk, .me.uk, você deve abrir um caso de suporte e solicitar proteção de privacidade.

Selecione Next (Próximo).

7. Na página Revisar, revise as informações que você inseriu, faça as correções necessárias. leia os termos de serviço e marque a caixa de seleção para confirmar que leu os termos de serviço.

   Selecione Enviar.

8. Somente para clientes da AISPL (Índia): Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para registrar um domínio no Route 53, execute as etapas a seguir para pagar a taxa de registro do domínio.

   a. Acesse a página Pedidos e faturas no AWS Management Console.
   b. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.
   c. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

      Depois de pagar a fatura, concluímos o registro de domínio e enviamos os e-mails aplicáveis.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para registrar um domínio após o cancelamento de uma fatura, reenvie a solicitação.

   Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

9. No painel de navegação, escolha Domínios e depois Solicitações.

   Nesta página, você pode ver o status do domínio e também se precisa responder ao e-mail de verificação do contato do registrante. Você também pode solicitar o reenvio do e-mail de verificação.

Se você especificou um endereço de e-mail de contato do registrante que nunca foi usado para registrar um domínio no Route 53, alguns registros TLD exigirão que você confirme que o endereço é válido.

Enviamos um e-mail de verificação de um dos seguintes endereços de e-mail:

- noreply@registrar.amazon.com: para TLDs registrados pelo Amazon Registrar.
- noreply@domainnameverification.net: para TLDs registrados por nosso associado registrador, Gandi. Para determinar quem é o registrador do seu TLD, consulte Como encontrar seu registrador.

> **Important**
>
> O contato inscrito deve seguir as instruções no e-mail para verificar se o e-mail foi recebido ou deveremos suspender o domínio conforme exigido pela ICANN. Quando um domínio é suspenso, não é possível acessá-lo na Internet.

a. Quando você receber o e-mail de verificação, escolha o link no e-mail que verifica se o endereço de e-mail é válido. Se você não receber o e-mail imediatamente, verifique sua pasta de lixo de e-mail.

b. Volte para a página Solicitações. Se o status não for atualizado automaticamente para dizer que o endereço de e-mail foi verificado, atualize o navegador.

10. Quando o registro do domínio estiver concluído, a próxima etapa dependerá da sua preferência pelo uso do Route 53 ou de outro serviço DNS para o domínio:

    - Route 53: na zona hospedada que o Route 53 criou quando você registrou o domínio, crie registros para informar ao Route 53 como deseja encaminhar o tráfego para o domínio e os subdomínios.

      Por exemplo, quando alguém insere o nome de seu domínio em um navegador e essa consulta é encaminhada ao Route 53, você deseja que o Route 53 responda à consulta com o endereço IP de um servidor Web em seu datacenter ou com o nome de um balanceador de carga do ELB?

      Para ter mais informações, consulte Trabalhar com registros.

> **Important**
>
> Se você criar registros em uma zona hospedada diferente daquela que o Route 53 cria automaticamente, deverá atualizar os servidores de nome do domínio para usar os servidores de nome da nova zona hospedada.

- Another DNS service (Outro serviço DNS): configure seu novo domínio para encaminhar consultas DNS para o outro serviço DNS. Execute o procedimento Atualizar servidores de nomes para usar outro registrador.

Valores que você especifica ao registrar ou transferir um domínio

> **Note**
>
> Atualizamos o console de domínios do Route 53. Durante o período de transição, você pode continuar a usar o console antigo ou pode usar o novo console. A maioria das informações retornadas pelo Route 53 é a mesma nos dois consoles. As diferenças estão anotadas na lista a seguir.

Ao registrar um domínio ou transferir o registro de um domínio para o Amazon Route 53, você especifica os valores que estão descritos neste tópico.

> **Note**
>
> Se você registrar mais de um domínio, o Route 53 usará os valores especificados para todos os domínios que estiverem no seu carrinho de compras.

Você também pode alterar os valores de um domínio que está atualmente registrado com o Route 53. Observe o seguinte:

- Se você alterar as informações de contato do domínio, enviaremos uma notificação por e-mail sobre a alteração ao contato registrante. Este e-mail vem de noreply@registrar.amazon. Para a maioria das alterações, o contato registrante não precisa responder.
- Para alterações nas informações de contato que também constituem uma alteração de proprietário, enviamos um e-mail adicional ao contato do registrante. A ICANN exige que o

contato registrante confirme que recebeu o e-mail. Para obter mais informações, consulte Nome, sobrenome e Organização mais adiante nesta seção.

Para obter mais informações sobre como alterar as configurações de um domínio existente, consulte Atualizar configurações de domínio .

Valores que você especifica

- 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

O mesmo que o contato do registrante

Especifica se você deseja usar as mesmas informações de contato para o registrante do domínio, o contato administrativo e o contato técnico.

Tipo de contato

Categoria deste contato. Observe o seguinte:

- Se você escolher uma opção diferente de Pessoa, deverá especificar o nome de uma organização.

- Para alguns TLDs, a proteção de privacidade disponível depende do valor escolhido para Tipo de contato. Para saber quais são as configurações de proteção de privacidade do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.
- Para domínios .es, o valor de Tipo de contato deve ser Pessoa para todos os três contatos.

Nome, sobrenome

O primeiro e o último nome do contato.

> **Important**
>
> Para First Name e Last Name, recomendamos que você especifique o nome no seu ID oficial. Para algumas alterações nas configurações de domínio, você deve comprovar sua identidade e o nome no seu ID deve coincidir com o nome do contato registrado do domínio.

Se você estiver transferindo um domínio para o Route 53 e o seguinte for true (verdadeiro), você estará alterando o proprietário do domínio:

- O tipo do contato é Person (Pessoa).
- Você está alterando os campos First Name (Nome) e/ou Last Name (Sobrenome) do contato registrante nas configurações atuais.

Nesse caso, a ICANN exige o envio de um e-mail ao contato registrante para obter aprovação. Enviamos um e-mail de um dos seguintes endereços de e-mail:

TLDs	Endereço de e-mail que envia o e-mail de aprovação
TLDs registrados pelo Amazon Registrar	noreply@registrar.amazon.com
.fr	nic@nic.fr (O e-mail é enviado aos contatos registrantes atual e novo.)
Todos os outros	noreply@domainnameverification.net

Para determinar quem é o registrador do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

> **Important**
>
> O contato do registrante deve seguir as instruções no e-mail, para confirmar que o e-mail foi recebido. Caso contrário, devemos suspender o domínio conforme exigido pela ICANN. Quando um domínio é suspenso, não é possível acessá-lo na Internet.

Se você alterar o endereço de e-mail do contato registrante, o e-mail será enviado aos endereços de e-mail anterior e atual do contato registrante.

Alguns registradores de TLD cobram uma taxa para alterar o proprietário do domínio. Quando você altera um desses valores, o console do Route 53 exibe uma mensagem indicando se há uma taxa.

Organização

A organização que está associada ao contato, se houver. Para os contatos registrante e administrativo, normalmente é a organização que está registrando o domínio. Para o contato técnico, ela pode ser a organização que gerencia o domínio.

Quando o tipo de contato é qualquer valor, exceto Pessoa, e você altera o campo Organização do contato registrante, o proprietário do domínio é alterado. A ICANN exige o envio de um e-mail ao contato registrante para obter aprovação. Enviamos um e-mail de um dos seguintes endereços de e-mail:

TLDs	Endereço de e-mail que envia o e-mail de aprovação
TLDs registrados pelo Amazon Registrar	noreply@registrar.amazon.com
.fr	nic@nic.fr (O e-mail é enviado aos contatos registrantes atual e novo.)
Todos os outros	noreply@domainnameverification.net

Para determinar quem é o registrador do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

Se você alterar o endereço de e-mail do contato registrante, o e-mail será enviado aos endereços de e-mail anterior e atual do contato registrante.

Alguns registradores de TLD cobram uma taxa para alterar o proprietário do domínio. Quando você altera o valor de Organization (Organização), o console do Route 53 exibe uma mensagem indicando se há uma taxa.

E-mail

O endereço de e-mail do contato.

Se você alterar o endereço de e-mail do contato registrante, enviaremos um e-mail de notificação aos endereços de e-mail anterior e atual. Este e-mail vem de noreply@registrar.amazon.

Telefone

O número de telefone do contato:

- Se você está informando um número de telefone de regiões dos Estados Unidos ou do Canadá, insira 1 no primeiro campo. Depois, insira o código de área de 10 dígitos e o número de telefone no segundo campo.
- Se você estiver informando um número de telefone de qualquer outro local, insira o código do país no primeiro campo e o restante do número de telefone no segundo campo. Para ver uma lista de códigos telefônicos de vários países, consulte o artigo da Wikipédia Lista de códigos telefônicos de vários países.

Endereço 1

O endereço do contato.

Endereço 2

Outras informações de endereço do contato, por exemplo, número do apartamento ou local de coleta de correspondências.

Country

O país do contato.

Estado

O estado ou a província do contato, se houver.

Cidade

A cidade do contato.

Código postal/CEP

O código postal do contato.

Campos para domínios de nível superior selecionados

Os domínios de nível superior (TLDs) a seguir exigem que você especifique outros valores:

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

Além disso, muitos TLDs exigem um número de identificação de IVA.

Para obter informações sobre valores válidos, consulte ExtraParama Referência de API do Amazon Route 53.

Proteção da privacidade

Se você deseja ocultar suas informações de contato de consultas WHOIS. Se você selecionar Desativar proteção de privacidade ou Ocultar informações de contato (console antigo), as consultas WHOIS ("quem é") retornarão informações de contato do registrador ou o valor "Protegido por política".

> **Note**
>
> Você deve especificar a mesma configuração de privacidade para os contatos administrativos, registrantes, técnicos e de cobrança.

Se você selecionar Não ocultar as informações de contato, receberá mais spam no endereço de e-mail que especificou.

Qualquer pessoa pode enviar uma consulta WHOIS para um domínio e receber todas as informações de contato desse domínio. O comando WHOIS está disponível em muitos sistemas operacionais e também como um aplicativo web em muitos sites.

> **Important**
>
> Embora haja usuários legítimos para as informações de contato associadas ao seu domínio, os usuários mais comuns são spammers que enviam aos contatos dos domínios e-mails indesejados e ofertas falsas. Em geral, recomendamos que você escolha Ocultar as informações de contato para Proteção de privacidade.

Para habilitar ou desabilitar a proteção de privacidade para alguns domínios, você deve abrir um caso de suporte e solicitar a proteção de privacidade.

Para obter mais informações sobre proteção de privacidade, consulte os tópicos a seguir:

- Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio
- Domínios que você pode registrar com o Amazon Route 53

Renovação automática (disponível somente ao editar as configurações do domínio)

Se você quiser que o Route 53 renove o domínio automaticamente antes que ele expire. A taxa de inscrição é cobrada em sua AWS conta. No console antigo, essa configuração só está disponível ao editar as configurações do domínio. Para ter mais informações, consulte Renovação do registro de um domínio.

> **Important**
>
> Se você desativar a renovação automática, o registro do domínio não será renovado quando a data de expiração passar e você poderá perder o controle do nome do domínio.

O período em que você pode renovar o nome de domínio varia de acordo com o domínio de nível superior (TLD). Para obter uma visão geral sobre como renovar domínios, consulte Renovação do registro de um domínio. Para obter informações sobre como estender o registro de domínio por um determinado número de anos, consulte Estender o período de registro de um domínio.

Valores que o Amazon Route 53 retorna quando você registra um domínio

Quando você registra seu domínio no Amazon Route 53, o Route 53 retorna os valores a seguir, além daqueles que você especificou.

Registrado em

A data em que o domínio foi originalmente registrado com o Route 53.

Expira em

A data e a hora em que o período de vigência do registro atual expira, no Tempo Médio de Greenwich (GMT).

O período de vigência do registro, normalmente, é de 1 ano, embora os registros de alguns domínios de nível superior (TLDs) tenham períodos mais longos. Para saber qual é o período de vigência do registro e renovação do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

Para a maioria dos TLDs, você pode estender o período de vigência do registro para até 10 anos. Para ter mais informações, consulte Estender o período de registro de um domínio.

Código de status do nome de domínio

O status atual do domínio.

A ICANN, a organização que mantém um banco de dados central de nomes de domínio, desenvolveu um conjunto de códigos de status de nomes de domínio (também conhecidos como códigos de status EPP), que informam o status de diversas operações em um nome de domínio. Por exemplo, registrar um nome de domínio, transferir um nome de domínio para outro reegistrador, renovar o registro de um nome de domínio etc. Todos os registradores usam esse mesmo conjunto de códigos de status.

Para ver uma lista atualizada de códigos de status de nomes de domínio e uma explicação do que cada código significa, acesse o site da ICANN e procure os códigos de status EPP. (Pesquise no site da ICANN; às vezes as pesquisas da Web retornam uma versão antiga do documento.)

Bloqueio de transferência

Determina se o domínio será bloqueado, para reduzir a possibilidade de alguém transferir seu domínio para outro registrador sem a sua permissão. Se o domínio estiver bloqueado, o valor

de Bloqueio de transferência será Ativado. Se o domínio não estiver bloqueado, o valor será Desativado.

Renovação automática

Determina se o Route 53 renovará automaticamente o registro desse domínio um pouco antes da data de validade.

Código de autorização

O código que será necessário se você quiser transferir o registro desse domínio para outro registrador. O código de autorização só será gerado quando você solicitar. Para obter informações sobre a transferência de um domínio para outro registrador, consulte Como transferir um domínio do Amazon Route 53 para outro registrador.

Servidores de nome

Os servidores do Route 53 que respondem a consultas de DNS para esse domínio. Recomendamos que você não exclua os servidores de nome do Route 53.

Para obter informações sobre como adicionar, alterar ou excluir servidores de nome, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

Visualizar o status do registro de um domínio

A ICANN, a organização que mantém um banco de dados central de nomes de domínio, desenvolveu um conjunto de códigos de status de nomes de domínio (também conhecidos como códigos de status EPP), que mostram o status de diversas operações, por exemplo, registrar um nome de domínio, transferir um nome de domínio para outro registrador, renovar o registro do nome de um domínio e assim por diante. Todos os registradores usam esse mesmo conjunto de códigos de status.

Para visualizar o código de status dos seus domínios, execute o procedimento a seguir.

Para visualizar o código de status da ICANN para um domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, expanda Domínios e escolha Domínios registrados.
3. Selecione o nome vinculado do seu domínio.

4. Se você precisar realizar uma ação, como reenviar o e-mail de verificação para o contato do registrante, um banner no alto da página indicará a ação que você precisa realizar.
5. Para o status atual do seu domínio, veja o valor do campo Código do status do domínio.

   Para ver uma lista atualizada de códigos de status de nomes de domínio e uma explicação do que cada código significa, acesse o site da ICANN e procure os códigos de status EPP. (Pesquise no site da ICANN; às vezes as pesquisas da Web retornam uma versão antiga do documento.)

Você também pode ver o status do registro na página Solicitações.

Para ver o status do registro

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios e escolha Solicitações.
3. Na página Solicitações, você pode ver o status do registro e também o status de todas as outras ações que você realizou nos domínios, como excluir domínios, bloquear transferências de domínios, adicionar ou excluir chaves do DNSSEC.

   Qualquer ação necessária para concluir um processo, como verificar seu e-mail, também estará listada.

   - Para responder a uma solicitação de ação, selecione o botão de opção ao lado do nome do domínio e selecione a ação no menu suspenso Ação.

Atualizar configurações de domínio

Para obter informações sobre como atualizar as configurações de um domínio, consulte o tópico aplicável.

Tópicos

- Atualizar informações de contato e propriedade de um domínio
- Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio
- Habilitar ou desabilitar a renovação automática de um domínio
- Bloquear um domínio para impedir uma transferência não autorizada para outro registrador

- Estender o período de registro de um domínio
- Atualizar servidores de nomes para usar outro registrador
- Adicionar ou alterar servidores de nome e registros cola de um domínio

Atualizar informações de contato e propriedade de um domínio

É possível alterar todas as informações dos contatos administrativos e técnicos de um domínio sem a necessidade de autorização para as mudanças. Para ter mais informações, consulte Atualizar informações de contato de um domínio.

É possível alterar a maioria dos valores dos contatos registrantes sem a necessidade de autorização para as mudanças. No entanto, para alguns TLDs, a alteração do proprietário de um domínio requer autorização. Para obter mais informações, consulte o tópico aplicável.

Tópicos

- Quem é o proprietário de um domínio?
- TLDs que exigem processamento especial para alterar o proprietário
- Atualizar informações de contato de um domínio
- Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio

Quem é o proprietário de um domínio?

Quando o tipo de contato é Pessoa e você altera os campos Nome ou Sobrenome do contato registrante, o proprietário do domínio é alterado.

Quando o tipo de contato é qualquer valor, exceto Pessoa, e você altera o campo Organização, o proprietário do domínio é alterado.

Em relação à alteração do proprietário de um domínio, atente-se ao seguinte:

- Para alguns TLDs, há uma taxa para alterar o proprietário de um domínio. Para determinar se há uma taxa para o TLD do seu domínio, consulte a coluna “Change Ownership Price” (Preço de alteração de propriedade) em Preço do Amazon Route 53 para registro de domínio.

> **Note**
>
> Você não pode usar AWS créditos para pagar a taxa, se houver, para alterar o proprietário de um domínio.

- Para alguns TLDs, quando você altera o proprietário de um domínio, nós enviamos um e-mail de autorização ao endereço de e-mail do contato do registrante. O contato registrante precisa seguir as instruções do e-mail para autorizar a mudança.
- Para alguns TLDs, é necessário preencher um formulário de alteração de propriedade do domínio e fornecer prova de identidade para que um engenheiro de suporte do Amazon Route 53 possa atualizar os valores para você. Se o TLD do seu domínio exigir o preenchimento de um formulário de alteração de propriedade de domínio, o console exibirá uma mensagem contendo um link para o formulário para abrir um caso junto ao suporte. Para ter mais informações, consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

TLDs que exigem processamento especial para alterar o proprietário

Quando você altera o proprietário de um domínio, os registros de alguns TLDs exigem processamento especial: Se você estiver alterando o proprietário de qualquer um dos domínios a seguir, execute o procedimento aplicável. Se estiver alterando o proprietário de qualquer outro domínio, você mesmo poderá alterá-lo de forma programática ou com o console do Route 53. Consulte Atualizar informações de contato de um domínio.

Os TLDs a seguir requerem processamento especial para alterar o proprietário do domínio:

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

.be

Você deve obter um código de transferência do registro para domínios.be e, em seguida, abrir um caso com o Support AWS .

- Para obter o código de transferência, consulte https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer e siga as instruções.
- Para abrir um caso, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

.cl

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.com.ar

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.com.br

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.es

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.fi

Inicie a alteração do proprietário no console do Route 53. Após iniciar a alteração, você receberá uma chave de transferência do portador do endereço de e-mail fi-domain-tech@traficom.fi. Depois de receber a chave, abra um caso de suporte com o AWS Support e compartilhe o código da chave conosco. Consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

.qa

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.ru

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.se

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

.sh

Você deve preencher e enviar um formulário para o AWS Support. Consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio.

Atualizar informações de contato de um domínio

Para atualizar as informações de contato de um domínio, realize o procedimento a seguir.

Para atualizar as informações de contato de um domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio cujas informações de contato você deseja atualizar.
4. Na guia Informações de contato, escolha Editar.
5. Se você estiver alterando o endereço de e-mail do contato registrante, execute as etapas a seguir. Se você não estiver alterando o endereço de e-mail do contato registrante, vá para a etapa 6.

   a. Altere apenas o endereço de e-mail do contato registrante. Não altere quaisquer outros valores para qualquer um dos contatos do domínio. Se você também quiser alterar outros valores, altere-os posteriormente no processo.

      Escolha Salvar alterações.

      Para verificar o novo endereço de e-mail, enviamos um e-mail de verificação para o novo endereço (se necessário para o TLD). Você deve escolher o link no e-mail para verificar se o novo endereço de e-mail é válido. Se a verificação for obrigatória, e você não verificar o novo endereço de e-mail, o Route 53 suspenderá o domínio, conforme exigido pela ICANN.

      Se você precisar que o e-mail de verificação seja reenviado, navegue até a página Domínios registrados, escolha o botão de opção ao lado do nome de domínio que você atualizou e escolha o nome do domínio que você está atualizando. No alerta Verificar seu e-mail para evitar a suspensão do domínio, escolha Enviar o e-mail novamente.

   b. Se você quiser alterar outros valores do solicitante do registro, do administrador, do técnico ou dos contatos de cobrança do domínio, volte para a etapa 1 e repita o procedimento.
6. Atualize os valores aplicáveis. Você também pode escolher Copiar contato do registrante para preencher automaticamente as mesmas informações inseridas para o contato do registrante. Para ter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

Dependendo do TLD do seu domínio e dos valores que você está alterando, o console poderá exibir a seguinte mensagem:

"Para alterar o nome ou organização registrante, abra um caso."

Se essa mensagem for exibida, interrompa este procedimento e consulte Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio para obter mais informações.

7. Selecione Save (Salvar).
8. Somente para clientes da AISPL (Índia): Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para alterar o proprietário de um domínio quando o registro de TLD cobrar uma taxa para alterar o proprietário, execute as etapas a seguir para pagar a taxa pela extensão.

   a. Acesse a página Pedidos e faturas no AWS Management Console.
   b. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.
   c. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

   Após o pagamento da fatura, alteraremos as configurações aplicáveis para o contato do registrante.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para alterar as configurações do contato do registrante após o cancelamento de uma fatura, reenvie a solicitação.

Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

9. Se você alterou o proprietário do domínio, conforme descrito em Quem é o proprietário de um domínio?, enviamos um e-mail para o contato do registrante do domínio. O e-mail solicita autorização para a alteração do proprietário.

   Se não recebermos autorização para a alteração dentro de 3 a 15 dias (dependendo do domínio de nível superior) cancelaremos o pedido, conforme exigido pela ICANN.

O e-mail será enviado de um dos seguintes endereços.

TLDs	Endereço de e-mail que envia a mensagem de autorização
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
Todos os outros	Um dos seguintes endereços de e-mail: • noreply@registrar.amazon.com • noreply@domainnameverification.net

10. Se você tiver problemas ao atualizar as informações de contato, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Para obter informações sobre a API que você pode usar para atualizar as informações de contato, consulte UpdateDomainContato.

Alterar o proprietário de um domínio quando o registro requer um formulário de alteração de propriedade de domínio

Se o registro do seu domínio exigir que você conclua uma Mudança de Propriedade do Domínio e envie o formulário para o AWS Support, execute o procedimento a seguir. Para determinar se você precisa executar esse procedimento, consulte os seguintes tópicos:

- Para determinar se o valor que você está alterando é considerado uma alteração de proprietário, consulte Quem é o proprietário de um domínio?.
- Para determinar se um formulário de Alteração de propriedade do domínio é necessário para o seu domínio, consulte TLDs que exigem processamento especial para alterar o proprietário.

Para alterar o proprietário de um domínio quando o registro exigir um formulário de alteração de propriedade do domínio

1. Consulte a introdução a este tópico para determinar se o registro do domínio requer processamento especial para alterar o proprietário do domínio. Se esse for o caso, e se um formulário de alteração de propriedade do domínio for obrigatório, continue com esse procedimento.

   Se não houver obrigatoriedade de formulário de alteração de propriedade do domínio, execute o procedimento no tópico aplicável.
2. Faça download do Formulário de alteração de propriedade do domínio. O arquivo é compactado em um arquivo.zip.
3. Preencha o formulário.
4. Para o contato do registrante do proprietário anterior do domínio e para o novo proprietário, obtenha uma cópia de uma prova de identidade assinada (carteira de identidade, carteira de habilitação, passaporte ou outra prova de identidade legal).

   Além disso, se uma pessoa jurídica estiver listada como a organização registrante, colete as seguintes informações do proprietário anterior do domínio e do novo proprietário:

   - Prova de que a organização com a qual o domínio está registrado existe.
   - Prova de que os representantes do proprietário anterior e o novo proprietário estão autorizados a agir em nome da organização. Esse documento precisa ser um documento certificado e legal que contenha o nome da organização e os nomes dos representantes como diretores assinantes (por exemplo, CEO, presidente ou diretor executivo).
5. Digitalize o formulário de alteração de propriedade do domínio e a prova necessária. Salve os documentos digitalizados em um formato comum, por exemplo, um .pdf ou .png.
6. Usando a AWS conta na qual o domínio está registrado atualmente, entre no AWS Support Center.

   Important

   Você deve fazer login usando a conta raiz ou um usuário que tenha recebido permissões do IAM de uma das seguintes formas:

   - A política AdministratorAccessgerenciada é atribuída ao usuário.
   - O usuário recebe a política gerenciada AmazonRoute53 DomainsFull Access.

- O usuário recebe a política FullAccess gerenciada AmazonRoute53.

Se você não fizer login usando a conta raiz ou um usuário que tenha as permissões necessárias, não poderemos atualizar o proprietário do domínio. Esse requisito impede que usuários não autorizados alterem o proprietário de um domínio.

7. Especifique os seguintes valores:

Referente

Aceite o valor padrão de Atendimento ao cliente.

Serviço

Aceite o valor padrão de Faturamento.

Categoria

Aceite o valor padrão de Problema no registro do nome do domínio.

Sujeito

Especifique Change the owner of a domain (Alterar o proprietário de um domínio).

Descrição

Forneça as informações a seguir:

- Domínio para o qual você deseja alterar o proprietário
- ID da conta de 12 dígitos da AWS conta na qual o domínio está registrado

Adicionar anexos

Faça upload dos documentos que você digitalizou na etapa 5.

Método de contato

Especifique um método de contato e insira os valores aplicáveis.

8. Selecione Enviar.

Um engenheiro do AWS Support analisa as informações que você forneceu e atualiza as configurações. O engenheiro entrará em contato com você quando a atualização for concluída ou para obter mais informações.

Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio

Quando você registra um domínio no Amazon Route 53 ou transfere um domínio para o Route 53, nós habilitamos a proteção de privacidade, por padrão, para todos os contatos do domínio. Geralmente, isso esconde a maioria das suas informações de contato das consultas WHOIS ("Who is" [quem é]) e reduz a quantidade de spam que você recebe. Ao habilitar a proteção de privacidade, suas informações de contato são substituídas pelas informações de contato do registrador ou pela frase "REDACTED FOR PRIVACY" (OCULTADO POR PRIVACIDADE) ou "On behalf of <domain name> owner" (Em nome do proprietário de <nome domínio>).

Se você optar por desabilitar a proteção de privacidade, será necessário desabilitá-la para todos os contatos de um domínio. Se você desabilitar a proteção de privacidade, qualquer pessoa poderá enviar uma consulta WHOIS para o domínio e, para a maioria dos domínios de nível superior (TLDs), obter todas as informações de contato fornecidas por você quando registrou ou transferiu o domínio, incluindo nome, endereço, número de telefone e endereço de e-mail. O comando WHOIS é amplamente disponível. Ele está incluído em muitos sistemas operacionais e também está disponível como aplicativo web em muitos sites.

Se você estiver transferindo um domínio para outro registro e a proteção de privacidade estiver ativada para os contatos do domínio, o e-mail para verificação da transferência será entregue pelos endereços identity-protect.org para TLDs registrados no Amazon Registrar. Para determinar quem é o registrador do seu TLD, consulte Como encontrar seu registrador.

As informações que você pode ocultar das consultas WHOIS dependem de dois fatores principais:

O registro do domínio de nível superior

A maioria dos registros de TLD escondem todas as informações de contato automaticamente, outros dão a opção de ocultar todas as informações de contato, de ocultar apenas algumas informações ou não permitem ocultar nenhuma informação.

Quando a proteção de privacidade em um domínio é habilitada, suas informações de contato são substituídas pelas informações de contato do serviço de privacidade) ou pela frase "REDACTED FOR PRIVACY" (OCULTADO POR PRIVACIDADE). O serviço de proteção de privacidade aplica recursos de prevenção de spam (alternação de endereços e análise de SPF/DKIM/spam) e, na maioria dos casos, encaminhará automaticamente os e-mails que passarem por esses filtros. No entanto, não é aconselhável enviar e-mails essenciais para endereços de e-mail protegidos pela privacidade, pois o mecanismo de spam pode impedir que eles sejam encaminhados.

Além disso, a escolha de qual mecanismo de proteção de privacidade é usado para um domínio não é configurável e é selecionada automaticamente pelo sistema. Os detalhes de contato do nosso serviço de proteção de privacidade não podem ser atualizados manualmente.

> **Note**
>
> Para habilitar ou desabilitar a proteção de privacidade para alguns domínios, você deve abrir um caso de suporte e solicitar a proteção de privacidade. Para obter mais informações, consulte a seção aplicável em Domínios que você pode registrar com o Amazon Route 53.
>
> - .co.uk (Reino Unido)
> - .me.uk (Reino Unido)
> - .org.uk (Reino Unido)
> - .link

O registrador

Quando você registra um domínio no Route 53 ou transfere um domínio para o Route 53, o registrador do domínio é o Amazon Registrar ou o nosso registrador associado, Gandi. Por padrão, o Amazon Registrar e o Gandi ocultam diferentes informações:

- Amazon Registrar: por padrão, todas as suas informações de contato ficam ocultas. No entanto, os regulamentos para o registro de TLD têm precedência.
- Gandi: por padrão, todas as suas informações de contato ficam ocultas, exceto o nome da organização, se houver. No entanto, os regulamentos para o registro de TLD têm precedência.

  Para TLDs geográficos que não permitem a proteção da privacidade, suas informações pessoais serão marcadas como "editadas" na página Whois Directory Search (Pesquisa de diretório Whois) no site da Gandi. No entanto, suas informações pessoais podem estar disponíveis no registro de domínio ou em sites WHOIS de terceiros.

Para descobrir quais informações ficam ocultas para o TLD do seu domínio, consulte Domínios que você pode registrar com o Amazon Route 53.

Quando quiser habilitar ou desabilitar a proteção de privacidade de um domínio que você registrou usando o Route 53, realize o procedimento a seguir.

Para habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio para o qual você deseja habilitar ou desabilitar a proteção de privacidade.
4. Na seção Informações de contato, escolha Editar.
5. Na seção Proteção de privacidade, escolha se deseja ocultar suas informações de contato. Você deve especificar a mesma configuração de privacidade para todos os quatro contatos: administrador, solicitante do registro, técnico e cobrança.

   > **Note**
   >
   > Se a proteção de privacidade não for compatível com o TLD, a seção Proteção de privacidade não será exibida.

6. Escolha Salvar alterações.
7. Se você encontrar problemas ao ativar ou desativar a proteção de privacidade, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Habilitar ou desabilitar a renovação automática de um domínio

Quando você quiser alterar a configuração do Amazon Route 53 para renovação automática do registro de um domínio pouco antes da data de validade, ou desejar ver a configuração atual para renovação automática, execute o seguinte procedimento.

Observe que você não pode usar AWS créditos para pagar a taxa de renovação do registro de um domínio.

> **Note**
>
> Certifique-se de desativar a renovação automática se você pretende cancelar sua AWS conta. Caso contrário, você continuará recebendo avisos de renovação de AWS. Porém, seu domínio não será renovado, a menos que você reative a conta.

Para habilitar ou desabilitar a renovação automática de um domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio que você deseja atualizar.
4. Na seção Detalhes, no menu suspenso Ações, escolha Ativar a renovação automática

   Em Ativar a renovação automática para <nome do domínio>?, concorde em pagar a taxa anual e escolha Ativar.

   > **Note**
   >
   > O preço listado é para o período de registro atual e pode mudar. Para obter mais informações, consulte Amazon Route 53 Pricing for Domain Registration.

5. Para desativar a renovação automática, selecione Desativar a renovação automática no menu suspenso Ações.
6. Se você tiver problemas ao ativar ou desativar a renovação automática, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Bloquear um domínio para impedir uma transferência não autorizada para outro registrador

Os registros de domínio para todos os TLDs genéricos e muitos dos TLDs geográficos permitem que você bloqueie um domínio para impedir que alguém transfira o domínio para outro registrador sem a sua permissão. Para determinar se o registro permite que você bloqueie o domínio, consulte Domínios que você pode registrar com o Amazon Route 53. Se o bloqueio for compatível e você quiser bloquear seu domínio, execute o procedimento a seguir. Você também pode usar o procedimento para desabilitar o bloqueio se deseja transferir um domínio para outro registrador.

Para bloquear um domínio e impedir uma transferência não autorizada para outro registrador

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.

3. Escolha o nome do domínio que você deseja atualizar.
4. Na seção Detalhes, no menu suspenso Ações, escolha Ativar bloqueio de transferência ou Desativar bloqueio de transferência, dependendo de você querer ativar ou desativar o bloqueio de transferência.

   Você pode navegar até a página Solicitações para ver o andamento de sua solicitação.
5. Se você encontrar problemas ao bloquear um domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Na pesquisa WHOIS, esse status aparece como: `clientTransferProhibited`. Além disso, alguns TLDs podem ter também estes status:

- `clientUpdateProhibited`
- `clientDeleteProhibited`

Estender o período de registro de um domínio

Quando você registra um domínio no Amazon Route 53 ou transfere o registro de um domínio para o Route 53, nós configuramos a renovação automática para o domínio. O período de renovação automática normalmente é de 1 ano, embora os registros de alguns domínios de nível superior (TLDs) tenham períodos de renovação mais longos.

Observe o seguinte:

Período máximo de renovação

Todos os TLDs genéricos e muitos dos TLDs de código de país permitem a extensão do registro de domínio por períodos mais longos (geralmente, até 10 anos com renovações anuais). Para saber se você pode estender o período de registro do seu domínio, consulte Domínios que você pode registrar com o Amazon Route 53. Se forem permitidos períodos de registro mais longos, realize o procedimento a seguir.

Restrições para quando você pode renovar ou estender um registro de domínio

Alguns registros de TLD têm restrições relacionadas a quando você pode renovar ou estender um registro de domínio. Por exemplo, nos últimos dois meses antes da expiração do domínio. Mesmo que a extensão do período de registro de um domínio seja permitida, pode haver restrições quanto ao número atual de dias que antecedem a expiração do domínio.

AWS créditos

Você não pode usar AWS créditos para pagar a taxa de extensão do período de registro de um domínio.

Para estender o período de registro do seu domínio

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio para o qual você deseja estender o período de registro.
4. Na seção Detalhes, no menu suspenso Ações, escolha Renovar registro de domínio.
5. Na caixa de diálogo Renovar registros de domínio, no menu suspenso Período de renovação, escolha por quantos anos você deseja estender o registro.

   A lista mostra todas as opções atuais com base na data de expiração atual e no período máximo de registro permitido pelo registro para o domínio em questão. A data de expiração com esse número de anos aplicado está listada em duração.
6. Escolha Renovar registro de domínio.

   Assim que recebermos a confirmação do registro referente à atualização da sua data de expiração, enviaremos um e-mail a você para confirmar essa mudança.
7. Somente para clientes da AISPL (Índia): Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para estender o registro de um domínio, execute as etapas a seguir para pagar a taxa pela extensão.

   a. Acesse a página Pedidos e faturas no AWS Management Console.
   b. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.
   c. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

      Após o pagamento da fatura, concluiremos a extensão e enviaremos os e-mails aplicáveis.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para estender o registro de domínio depois que uma fatura é cancelada, reenvie a solicitação.

Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

8. Se você tiver problemas ao estender o período de registro de um domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Atualizar servidores de nomes para usar outro registrador

Se você quiser passar o gerenciamento de DNS para outro registrador, precisará atualizar os servidores de nomes para apontar para

Para atualizar os servidores de nome do seu domínio quando você quiser usar outro serviço DNS

1. Use o processo fornecido pelo seu serviço DNS para obter os servidores de nome do domínio.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Domínios registrados.
4. Escolha o nome do domínio que você deseja configurar para usar outro serviço DNS.
5. Na seção Detalhes, no menu suspenso Ações, escolha Editar servidores de nomes.
6. Exclua os servidores de nomes existentes e adicione os nomes dos servidores de nomes aos servidores de nomes obtidos do serviço DNS na etapa 1.
7. Escolha Salvar alterações.
8. (Opcional) Exclua a zona hospedada que o Route 53 criou automaticamente quando você registrou o domínio. Isso evita que você seja cobrado por uma zona hospedada que não está usando.

    a. No painel de navegação, escolha Zonas hospedadas.

    b. Selecione o botão de opção da zona hospedada com o mesmo nome que o seu domínio.

    c. Escolha Excluir zona hospedada.

    d. Escolha Confirmar, para confirmar que você deseja excluir a zona hospedada.

Adicionar ou alterar servidores de nome e registros cola de um domínio

Quando você registra um domínio no Route 53, automaticamente criamos uma zona hospedada para o domínio, atribuímos quatro servidores de nome para a zona hospedada e atualizamos o registro do domínio para usar os servidores de nome. Normalmente, você não precisa alterar essas configurações, a menos que você queira usar outro serviço DNS ou usar servidores de nome de rótulo branco.

O número máximo de servidores de nomes por domínio no Route 53 é seis.

> **Warning**
>
> Se você alterar os servidores de nome para valores incorretos, especificar endereços IP incorretos nos registros cola ou excluir um ou mais servidores de nome sem especificar novos, seu site ou aplicativo poderá ficar indisponível na Internet por até dois dias.

Tópicos

Considerações para alterar servidores de nome e registros cola

Considere os seguintes problemas antes de alterar sua configuração.

Tópicos

Você quer tornar o Route 53 o serviço DNS para seu domínio

Se você estiver usando outro serviço DNS e desejar tornar o Route 53 o serviço DNS para seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente para obter instruções detalhadas sobre como migrar o serviço DNS para o Route 53.

> **Important**
>
> Se você não seguir rigorosamente o processo de migração, seu domínio pode ficar indisponível na Internet por até dois dias.

Você quer usar outro serviço DNS

Se você quiser usar um serviço DNS diferente do Route 53 para seu domínio, use o procedimento a seguir para alterar os servidores de nome do registro do domínio para os servidores de nome fornecidos pelo outro serviço DNS.

> **Note**
>
> Se você alterar os servidores de nome e o Route 53 retornar a mensagem de erro a seguir, o registro do TLD não reconhecerá os servidores de nome que você especificou como servidores de nome válidos:
> `"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."`
> Os registros de TLD normalmente são compatíveis com servidores de nome fornecidos por serviços DNS públicos, mas não são compatíveis com servidores DNS privados, como servidores DNS que você configurou em instâncias do Amazon EC2, a menos que o registro tenha endereços IP para esses servidores de nome. O Route 53 não suporta o uso de servidores de nomes que não são reconhecidos pelo registro TLD. Se encontrar esse erro, altere para servidores de nome para o Route 53 ou outro serviço DNS público.

Para usar servidores de nome de rótulo branco

Se desejar que os nomes de seus servidores de nome sejam subdomínios do nome de seu domínio, você poderá criar servidores de nome de rótulo branco. (Servidores de nome de rótulo branco também são conhecidos como servidores de nome privados ou servidores de nome intuitivos.) Por exemplo, você pode criar servidores de nome ns1.exemplo.com a ns4.exemplo.com para o domínio exemplo.com. Para usar os servidores de nome de rótulo branco, use o procedimento a seguir para especificar os endereços IP dos servidores de nome em vez dos nomes. Esses endereços IP são conhecidos como registros cola.

Para obter mais informações sobre como configurar servidores de nome de rótulo branco, consulte Configurar servidores de nome de rótulo branco.

Você está alterando servidores de nome para um domínio .it

Se você alterar servidores de nome para um domínio .it, o registro para domínios .it executará uma verificação para confirmar se os servidores de nome são válidos. Se você especificar os servidores de nome incorretos e a verificação falhar, o registro continuará verificando durante 22 dias. Durante esse período, não será possível atualizar os nomes dos servidores de nome para corrigir o erro pois o código de status EPP será `pendingUpdate`. O registro continua a responder às consultas DNS usando os servidores de nome anteriores à alteração. Se os servidores de nome anteriores não estiverem mais disponíveis, seu domínio ficará indisponível na Internet.

> **Important**
>
> Sempre que você alterar os servidores de nome de um domínio, confirme se o DNS está respondendo às consultas com os novos servidores de nome antes de cancelar o serviço DNS antigo ou excluir a zona hospedada do Route 53 que usou os servidores de nome antigos.

Para obter informações sobre como obter ajuda AWS para corrigir os nomes dos seus servidores de nomes com o registro de domínios.it, consulte. Entrar em contato com o AWS Support sobre problemas de registro de domínio

Adicionar ou alterar servidores de nome ou registros cola

Para adicionar ou alterar servidores de nome ou registros cola, siga o procedimento a seguir.

> **Note**
>
> Por padrão, os resolvedores DNS normalmente armazenam em cache os nomes dos servidores de nomes por dois dias. Como resultado, suas alterações podem levar dois dias para entrar em vigor. Para ter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

Para adicionar ou alterar servidores de nome ou registros cola de um domínio

1. Analise Considerações para alterar servidores de nome e registros cola e resolva os problemas aplicáveis, se houver.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Domínios registrados.
4. Escolha o nome do domínio para o qual você deseja editar as configurações.
5. Na seção Detalhes, no menu suspenso Ações, escolha Editar servidores de nomes.
6. Na caixa de diálogo Editar servidores de nomes, é possível fazer o seguinte:

   - Para alterar o serviço DNS do domínio, realize um dos seguintes procedimentos:
     - Substitua os servidores de nome de outro serviço DNS pelos servidores de nome de uma zona hospedada do Route 53
     - Substitua os servidores de nome de uma zona hospedada do Route 53 pelos servidores de nome de outro serviço DNS
     - Substitua os servidores de nome de uma zona hospedada do Route 53 pelos servidores de nome de outra zona hospedada do Route 53

     Para obter informações sobre como alterar o serviço DNS de um domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente. Para obter informações sobre como obter os servidores de nome para a zona hospedada do Route 53 que você deseja usar para o serviço DNS do domínio, consulte Obter os servidores de nome de uma zona hospedada pública.
   - Adicionar um ou mais servidores de nome.
   - Substituir o nome de um servidor de nome existente.
   - Se você especificar os servidores de nome de rótulo branco, adicione ou altere os endereços IP nos registros cola. É possível inserir endereços no formato IPv4 ou IPv6. Se um servidor de nome tiver vários endereços IP, insira cada endereço em uma linha separada.

     Um servidor de nome de rótulo branco inclui o seu nome de domínio, como example.com, no nome do servidor de nome, como ns1.exemplo.com. Quando você especifica um servidor de nome de rótulo branco, o Route 53 solicitará que você especifique um ou mais endereços IP para o servidor de nome. O endereço IP é conhecido como um registro cola. Para ter mais informações, consulte Configurar servidores de nome de rótulo branco.

- Excluir um servidor de nome. Escolha o ícone de x à direita do campo desse servidor de nome.

> **Warning**
>
> Se você alterar os servidores de nome para valores incorretos, especificar endereços IP incorretos nos registros cola ou excluir um ou mais servidores de nome sem especificar novos, seu site ou aplicativo poderá ficar indisponível na Internet por até dois dias.

7. Selecione Atualizar.
8. Se você tiver problemas ao adicionar ou alterar servidores de nomes ou registros do Glue, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Renovação do registro de um domínio

Quando você registra um domínio no Amazon Route 53 ou transfere o registro de um domínio para o Route 53, nós configuramos a renovação automática para o domínio. O período de renovação automática normalmente é de 1 ano, embora os registros de alguns domínios de nível superior (TLDs) tenham períodos de renovação mais longos. Para saber qual é o período de vigência do registro e renovação do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

> **Note**
>
> Você não pode usar AWS créditos para pagar a taxa de renovação do registro de um domínio.

Para a maioria dos domínios de nível superior (TLDs), você pode alterar a data de expiração de um domínio. Para ter mais informações, consulte Estender o período de registro de um domínio.

> **Important**
>
> Se você desativar a renovação automática, lembre-se dos seguintes efeitos no seu domínio:

- Alguns registros de TLD excluem domínios até mesmo antes da data de expiração, se você não renovar com antecedência suficiente. Se você deseja manter um nome de domínio, recomendamos que deixe a renovação automática ativada.
- Também é altamente recomendável que você não registre novamente um domínio depois que ele expirar. Alguns registradores permitem que outras pessoas registrem domínios imediatamente depois que eles expiram. Portanto, é possível que você não consiga registrar o domínio novamente antes que ele seja registrado por outra pessoa.
- Alguns registros cobram um valor alto para restaurar domínios expirados.
- Na data de expiração ou perto dela, o domínio se torna indisponível na Internet.

Para determinar se a renovação automática está ativada para o seu domínio, consulte Habilitar ou desabilitar a renovação automática de um domínio.

Se a renovação automática estiver ativada, veja o que acontecerá:

45 dias antes da validade

Enviamos um e-mail ao contato registrante informando que a renovação automática está ativada e com instruções sobre como desativá-la. Mantenha seu endereço de e-mail de contato registrante atualizado para não perder esse e-mail.

35 ou 30 dias antes da validade

Para todos os domínios, exceto domínios .com.ar, .com.br e .jp, renovamos o registro do domínio 35 dias antes da data de expiração, para termos tempo de resolver todos os problemas com a sua renovação antes que o nome de domínio expire.

Os registros dos domínios .com.ar, .com.br e .jp requerem a renovação dos domínios no mínimo 30 dias antes da validade. Você receberá um e-mail de renovação de Gandi, nosso associado registrador, 30 dias antes da expiração, ou seja, no mesmo dia em que renovaremos seu domínio, se a renovação automática estiver ativada.

> **Note**
>
> Quando seu domínio for renovado, enviaremos um e-mail para informá-lo sobre isso. Se a renovação falhar, enviaremos um e-mail para explicar o motivo.

Se a renovação automática estiver desativada, veja o que acontecerá, à medida que a data de expiração de um nome de domínio se aproximar:

45 dias antes da validade

Enviamos um e-mail ao contato registrante do domínio, informando que a renovação automática está desativada e com instruções sobre como ativá-la. Mantenha seu endereço de e-mail de contato registrante atualizado para não perder esse e-mail.

30 e 7 dias antes da expiração

Se a renovação automática estiver desativada para o domínio, a ICANN, o órgão que rege o registro de domínios, exigirá que o registrador envie um e-mail a você. O e-mail será enviado de um dos seguintes endereços:

- noreply@registrar.amazon.com : para domínios cujo registrador é o Amazon Registrar.
- noreply@domainnameverification.net: para domínios cujo registrador é nosso registrador associado, Gandi.

Para determinar quem é o registrador do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

Se você ativar a renovação automática menos de 30 dias antes da data de expiração e o período de renovação não tiver passado, o domínio será renovado em até 24 horas.

> **Important**
>
> Alguns registros de TLDs deixam de permitir renovações até 25 dias antes da data de expiração, e muitos não permitem a renovação após a data de expiração. Além disso, o processamento de uma renovação pode levar até um dia. Se você demorar muito para ativar a renovação automática, o domínio poderá expirar antes do processamento da renovação, e você poderá perder o domínio. Se a data de expiração estiver se aproximando, recomendamos que você a estenda manualmente para o domínio. Para ter mais informações, consulte Estender o período de registro de um domínio.

Para obter mais informações sobre períodos de renovação, consulte a seção Deadlines for renewing and restoring domains para seu TLD na Domínios que você pode registrar com o Amazon Route 53.

Após a data de validade

A maioria dos domínios é mantida pelo registrador por um breve período após a expiração. Portanto, é possível que você consiga renovar um domínio expirado após a data de expiração, mas recomendamos que mantenha a renovação automática ativada se quiser manter o seu domínio. Para obter informações sobre como tentar renovar um domínio após a data de expiração, consulte Restaurar um domínio expirado ou excluído.

Se o seu domínio expirar, mas a renovação com atraso for permitida para o domínio, você poderá renovar o domínio pelo preço de renovação padrão. Para determinar se um domínio ainda está dentro do período de renovação com atraso, execute o procedimento na seção Estender o período de registro de um domínio. Se o domínio ainda estiver listado, ele estará dentro do período de renovação com atraso.

Para obter mais informações sobre períodos de renovação, consulte a seção Deadlines for renewing and restoring domains para seu TLD na Domínios que você pode registrar com o Amazon Route 53.

Restaurar um domínio expirado ou excluído

Se você não renovar um domínio antes do fim do período de renovação com atraso ou se excluir acidentalmente o domínio, alguns registros para domínios de nível superior (TLDs) permitem que você restaure o domínio antes que ele seja disponibilizado para ser registrado por outras pessoas.

Quando um domínio é excluído ou passa do fim do período de renovação com atraso, ele não aparece mais no console do Amazon Route 53.

> **Important**
>
> O preço para restaurar um domínio é geralmente mais alto e, às vezes, muito mais alto que o preço para registrar ou renovar um domínio. Para obter o preço atual da restauração de um domínio, consulte a coluna Restoration Price em Amazon Route 53 Pricing for Domain Registration.

Você não pode usar AWS créditos para pagar a taxa de restauração de um domínio expirado.

Para tentar restaurar o registro de domínio quando um domínio é excluído ou o período de renovação com atraso expirou

1. Determine se o registro do TLD do domínio é compatível com a restauração de domínios e, se esse for o caso, o período durante o qual a restauração é permitida.

   a. Acesse Domínios que você pode registrar com o Amazon Route 53.

   b. Encontre o TLD do seu domínio e revise os valores na seção Deadlines for renewing and restoring domains.

   > **Important**
   >
   > Encaminhamos as solicitações de restauração à Gandi, que as processa durante o horário comercial, de segunda a sexta-feira. A Gandi fica em Paris, onde o fuso horário é UTC/GMT + 1 hora. Como resultado, dependendo de quando você envia sua solicitação, em casos raros pode demorar uma semana ou mais para que uma solicitação seja processada.

2. Revise o preço para restaurar um domínio, que é geralmente mais alto e, às vezes, muito mais alto que o preço para registrar ou renovar um domínio. Em Amazon Route 53 Pricing for Domain Registration, encontre o TLD do domínio (como .com) e verifique o preço na coluna Restoration Price. Se ainda deseja restaurar o domínio, anote o preço; você precisará dele em uma etapa posterior.
3. Usando a AWS conta na qual o domínio foi registrado, entre no AWS Support Center.
4. Especifique os seguintes valores:

   Referente

   Aceite o valor padrão de Atendimento ao cliente.

   Serviço

   Aceite o valor padrão de Faturamento.

   Categoria

   Aceite o valor padrão de Problema no registro do nome do domínio.

Sujeito

Insira Restore an expired domain (Restaurar um domínio expirado) ou Restore a deleted domain (Restaurar um domínio excluído).

Descrição

Forneça as informações a seguir:

- O domínio que você deseja restaurar
- O ID da conta de 12 dígitos da AWS conta na qual o domínio foi registrado
- Confirmação de que você aceita o preço para restaurar o domínio. Use o seguinte texto:

  "Concordo com o preço de ____ USD para restaurar meu domínio."

  Substitua o espaço em branco pelo preço que você encontrou na etapa 2.

Método de contato

Especifique um método de contato e, se você escolher Telefone, insira os valores aplicáveis.

5. Selecione Enviar.
6. Quando soubermos se conseguimos restaurar seu domínio, um representante do AWS Support entrará em contato com você. Além disso, se pudermos restaurar o domínio, ele será exibido novamente no console com a nova data de expiração. A data de expiração depende se o domínio expirou ou foi excluído acidentalmente:

   O domínio expirou

   A nova data de expiração geralmente é de um ou dois anos (dependendo do TLD) após a data de expiração antiga.

   > **Note**
   >
   > A nova data de expiração não é calculada a partir da data em que o domínio foi restaurado.

   O domínio foi excluído acidentalmente

   Normalmente, a data de expiração não muda.

Como substituir a zona hospedada por um domínio registrado com o Route 53

Se você excluir a zona hospedada de um domínio, precisará criar outra zona hospedada quando estiver pronto para disponibilizar o domínio na Internet. Execute o procedimento a seguir.

Para substituir a zona hospedada de um domínio

1. Crie uma zona hospedada pública. Para ter mais informações, consulte Criar uma zona hospedada pública.
2. Crie registros na zona hospedada. Os registros definem como você quer rotear o tráfego para o domínio (example.com) e subdomínios (acme.example.com, zenith.example.com). Para ter mais informações, consulte Trabalhar com registros.
3. Atualize a configuração do domínio para usar os servidores de nome da nova zona hospedada. Para ter mais informações, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

   > **Important**
   >
   > Quando você cria uma zona hospedada, o Route 53 atribui um conjunto de quatro servidores de nome à zona hospedada. Se você excluir uma zona hospedada e depois criar uma nova, o Route 53 atribuirá outro conjunto de quatro servidores de nomes. Geralmente, nenhum dos servidores de nome da nova zona hospedada corresponde a nenhum dos servidores de nome da zona hospedada anterior. Se você não atualizar a configuração do domínio para usar os servidores de nome da nova zona hospedada, o domínio permanecerá indisponível na Internet.

4. Se você encontrar problemas ao substituir a zona hospedada por um domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Transferir domínios

É possível transferir o registro de domínio de outro registrador para o Amazon Route 53, de uma conta da AWS para outra ou do Route 53 para outro registrador. Não há custo para transferir domínios de uma AWS conta para outra.

Tópicos

Como transferir registro de um domínio para o Amazon Route 53

> **Important**
>
> Durante a transferência de qualquer domínio de primeiro nível com código de país (ccTLDs) para o Route 53, exceto o.cc e .tv, as atualizações do contato do proprietário são ignoradas e os dados de contato do proprietário do registro são usados. Você pode atualizar o contato do proprietário após a conclusão da transferência. Para ter mais informações, consulte Atualizar informações de contato e propriedade de um domínio.

Para transferir o registro de um domínio para o Amazon Route 53, siga os procedimentos deste tópico.

> **Important**
>
> Se você pular uma etapa, seu domínio poderá se tornar indisponível na Internet.

Observe o seguinte:

Entrando em contato com AWS o Suporte

Se você tiver problemas ao transferir um domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Data de validade

Para obter informações sobre como transferir seu domínio afeta a data de expiração atual, consulte Como a transferência de um domínio para o Amazon Route 53 afeta a data de validade do seu registro de domínio.

Taxa de transferência

Quando você transfere um domínio para o Route 53, a taxa de transferência que aplicamos à sua AWS conta depende do domínio de nível superior, como .com ou .org. Para obter mais informações, consulte Preço do Route 53.

Você não pode usar AWS créditos para pagar a taxa, se houver, pela transferência de um domínio para o Route 53.

> **Note**
>
> O Route 53 cobra a taxa de transferência do seu domínio antes de iniciarmos o processo de transferência. Se uma transferência falhar por algum motivo, efetuaremos o crédito pelo custo da transferência em sua conta imediatamente.

Nomes de domínio premium e especiais

Os registros de TLD atribuíram preços especiais ou premium a alguns nomes de domínio. Não será possível transferir um domínio para o Route 53, se ele tiver um preço especial ou premium.

Cotas do domínio

O número máximo padrão de domínios por AWS conta é 20. É possível solicitar uma cota maior. Para ter mais informações, consulte Cotas em domínios.

Limite dos servidores de nomes

O número máximo de servidores de nomes por domínio no Route 53 é seis.

Tópicos

- Requisitos de transferência para domínios de nível superior
- Etapa 1: Confirmar que o Amazon Route 53 oferece suporte ao domínio de nível superior
- Etapa 2 (opcional): transferir o serviço DNS para o Amazon Route 53 ou outro provedor de serviços DNS

- Etapa 3: alterar as configurações com o registrador atual
- Etapa 4: obter os nomes dos seus servidores de nome
- Etapa 5: solicitar a transferência
- Etapa 6: apenas clientes da AISPL (Índia): pagar a taxa de transferência
- Etapa 7: clicar no link nos e-mails de confirmação e autorização
- Etapa 8: atualizar a configuração do domínio

Requisitos de transferência para domínios de nível superior

A maioria dos registradores de domínio impõe requisitos sobre a transferência de um domínio para outro registrador. O objetivo principal desses requisitos é impedir que os proprietários de domínios fraudulentos transfiram repetidamente os domínios para diferentes registradores. Os requisitos variam, mas os seguintes requisitos são típicos:

- Você deve ter registrado o domínio com o registrador atual ou transferido o registro do domínio para o registrador atual há pelo menos 60 dias.
- Se o registro de um nome de domínio expirou e precisou ser restaurado, ele deve ter sido restaurado há pelo menos 60 dias.
- O domínio não pode ter qualquer um dos seguintes códigos de status de nome de domínio:
  - cliente TransferProhibited
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - servidor TransferProhibited
- Os registros de alguns domínios de nível superior não permitem transferências até que as alterações estejam concluídas, como alterações no proprietário do domínio.

Para ver uma lista atualizada de códigos de status de nomes de domínio e uma explicação do significado de cada código, visite o site da ICANN e pesquise os códigos de status EPP. (Pesquise no site da ICANN; às vezes as pesquisas da Web retornam uma versão antiga do documento.)

> **Note**
>
> A ICANN é a organização que estabelece as políticas que controlam o registro e a transferência de nomes de domínio.

Você também pode pesquisar seu nome de domínio no site da Whois para ver códigos de status e outras informações do seu domínio.

Etapa 1: Confirmar que o Amazon Route 53 oferece suporte ao domínio de nível superior

Consulte Domínios que você pode registrar com o Amazon Route 53. Se o domínio de nível superior do domínio que você deseja transferir estiver na lista, será possível transferi-lo para o Amazon Route 53.

Se um TLD não estiver na lista, no momento você não poderá transferir o registro de domínio para o Route 53. Ocasionalmente, nós adicionamos mais TLDs à lista. Portanto, verifique se adicionamos suporte ao seu domínio.

Etapa 2 (opcional): transferir o serviço DNS para o Amazon Route 53 ou outro provedor de serviços DNS

Por que transferir o DNS primeiro?

Algumas empresas de registro de domínio fornecem serviço DNS gratuito que pode ser desabilitado assim que recebem uma solicitação do Route 53 para transferir o registro do domínio. Se pretende que o Route 53 forneça o serviço DNS para o seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Etapa 3: alterar as configurações com o registrador atual

Usando o método fornecido pelo registrador atual, execute as seguintes tarefas para cada domínio que você quer transferir.

- 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)

Confirme se o e-mail do contato do registrante do seu domínio está atualizado

Enviaremos uma mensagem para esse endereço de e-mail a fim de solicitar autorização para a transferência. Você precisa clicar em um link no e-mail para autorizar a transferência. Se você não clicar no link, devemos cancelar a transferência.

Desbloqueie o domínio para que ele possa ser transferido

A ICANN, órgão que rege o registro de domínios, exige que você desbloqueie o seu domínio antes de transferi-lo.

Confirme se o status do domínio permite que você transfira o domínio

Para ter mais informações, consulte Requisitos de transferência para domínios de nível superior.

Desabilitar o DNSSEC para o domínio

Se você usar o DNSSEC com um domínio e transferir o registro de domínio para o Route 53, será necessário desabilitar primeiro o DNSSEC no antigo registrador. Em seguida, depois de transferir o registro de domínio, siga passos para configurar o DNSSEC para o domínio no Route 53. O Route 53 oferece suporte ao DNSSEC com o registro de domínios, mas não para o DNS. Para ter mais informações, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

> **Important**
>
> Se você transferir um registro de domínio para o Route 53 enquanto o DNSSEC estiver configurado, as chaves públicas DNSSEC também serão transferidas. Se você transferir o serviço DNS para um provedor que não ofereça suporte ao DNSSEC, a resolução DNS falhará, de forma intermitente, até que você elimine as chaves DNSSEC do domínio. Para ter mais informações, consulte Excluir chaves públicas de um domínio.

Obter um código de autorização

Um código de autorização do registrador atual nos autoriza a solicitar que o registro do domínio seja transferido para o Route 53. Você vai inserir esse código no console do Route 53 mais adiante no processo.

Alguns domínios de nível superior têm requisitos adicionais:

Domínios .co.za

Não é necessário obter um código de autorização para transferir um domínio .co.za ao Route 53.

Domínios .es

Se você estiver transferindo um domínio .es para o Route 53, não será necessário obter um código de autorização.

domínios .uk, .co.uk, .me.uk e .org.uk

Se estiver transferindo um domínio .uk, .co.uk, .me.uk ou .org.uk para o Route 53, não será necessário obter um código de autorização. Em vez disso, use o método fornecido pelo registrador de domínio atual para atualizar o valor da tag de IPS do domínio para GANDI, tudo em letras maiúsculas. (Uma tag de IPS é exigida pelo Nominet, entidade responsável pela gestão dos domínios .uk.) Se o seu registrador não oferecer uma maneira de alterar o valor da tag IPS, entre em contato com a Nominet.

Observe o seguinte em relação à alteração da tag IPS:

Você deve solicitar a transferência em até cinco dias

Se você não solicitar a transferência em até cinco dias depois de alterar a tag IPS, a tag será alterada de volta para o valor anterior. É necessário alterar o valor da tag IPS novamente, caso contrário, ocorrerá uma falha na solicitação de transferência.

Visualizar a tag IPS em consultas WHOIS

A alteração na tag IPS não aparece nas consultas WHOIS até que a transferência para o Route 53 tenha sido concluída.

E-mail do Gandi

Você poderá receber um e-mail do nosso registrador associado, o Gandi, sobre o processo de transferência. Se você receber um e-mail do Gandi (transfer-auth@gandi.net) sobre como transferir seu domínio, ignore as instruções no e-mail, pois elas não são relevantes para o Route 53. Em vez disso, siga as instruções deste tópico.

Renovar o seu registro de domínio antes de transferir o domínio (TLDs geográficos selecionados)

Para a maioria dos TLDs, quando você transferir um domínio, o registro será renovado automaticamente por um ano. No entanto, para alguns TLDs geográficos, o registro não é

estendido quando você transfere o domínio. Se você estiver transferindo um domínio para o Route 53 que tenha um desses TLDs, recomendamos que você renove o registro de domínio antes de transferir o domínio, especialmente se a data de validade estiver se aproximando.

> **Important**
>
> Se você não renovar o domínio antes de transferi-lo, o registro pode expirar antes que a transferência seja concluída. Se isso acontecer, o domínio se torna indisponível na Internet e o nome de domínio pode ser disponibilizado para compra por outras pessoas.

O registro não será renovado automaticamente quando você transferir os seguintes domínios para outro registrador:

- .ch (Suíça)
- .cl (Chile)
- .co.uk (Reino Unido)
- .co.za (África do Sul)
- .com.au (Austrália)
- .cz (República Tcheca)
- .es (Espanha)
- .fi (Finlândia)
- .im (Ilha de Man)
- JP (Japão)
- .me.uk (Reino Unido)
- .net.au (Austrália)
- .org.uk (Reino Unido)
- .se (Suécia)
- .uk (Reino Unido)

Etapa 4: obter os nomes dos seus servidores de nome

Se você estiver usando o Amazon Route 53 como seu serviço DNS ou se continuar usando o serviço DNS existente, nós obteremos os nomes dos servidores de nome para você automaticamente mais adiante no processo. Vá para Etapa 5: solicitar a transferência.

Se você quiser alterar o serviço DNS para outro provedor que não seja o Route 53 ao mesmo tempo em que transfere o domínio para o Route 53, use o procedimento fornecido pelo provedor de serviço DNS para obter os nomes dos servidores de nome de cada domínio que quer transferir.

> **Important**
>
> Se o registrador de seu domínio também for o provedor de serviços DNS do domínio, transfira o serviço DNS para o Route 53 ou para outro provedor de serviços DNS antes de continuar o processo de transferência do registro do domínio.
> Se você transferir o serviço de DNS ao mesmo tempo em que transfere o registro de domínio, seu site, e-mail e aplicativos web associados ao domínio poderão ficar indisponíveis. Para ter mais informações, consulte Etapa 2 (opcional): transferir o serviço DNS para o Amazon Route 53 ou outro provedor de serviços DNS.

Etapa 5: solicitar a transferência

Para transferir o registro de domínio do registrador atual ao Amazon Route 53, use o console do Route 53 para solicitar a transferência. O Route 53 faz a comunicação com o registrador atual do domínio.

Você pode usar o console para transferir até cinco domínios.

O procedimento que você usa depende de você querer transferir até cinco domínios ou mais de cinco domínios:

- Para transferir o registro de um único domínio para o Route 53
- Transferir o registro de domínio para o Route 53 para até cinco domínios

Use o processo Transferir domínio para sua conta para transferir um único domínio para sua conta.

Para transferir o registro de um único domínio para o Route 53

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Na página Domínios registrados, escolha Domínio único no menu suspenso Transfência de entrada.

4. Na página Transferir domínio para sua conta, na seção Verificar transferibilidade do domínio, insira o nome do domínio cujo registro você deseja transferir para o Route 53 e escolha Verificar.
5. Se o registro do domínio estiver disponível para transferência, verifique se você cumpriu os requisitos de transferência para domínios de nível superior e escolha Avançar.

   Se o registro do domínio não estiver disponível para transferência, o console do Route 53 listará os motivos. Entre em contato com o registrador para obter informações sobre como resolver os problemas o impedem de transferir o registro.
6. Na página Serviço DNS, revise as informações sobre servidores de nomes e escolha Avançar.
7. Se solicitado, insira o código de autorização ou a tag IPS que você obteve do registrador atual em Etapa 3: alterar as configurações com o registrador atual.

   > **Note**
   >
   > Não é necessário inserir um código de autorização para transferir um domínio .co.za, .es, .uk, .co.uk, .me.uk ou .org.uk para o Route 53.

   Selecione Next (Próximo).
8. Na página Opções de preços de domínio, escolha por quantos anos você deseja registrar o domínio para o qual você está transferindo e se deseja que renovemos automaticamente o registro do domínio antes da data de expiração.

   > **Note**
   >
   > Os registros e as renovações de nome de domínio não são restituíveis. Se você habilitar a renovação automática do domínio e decidir que não deseja o nome de domínio depois de renovar o registro, não poderá receber reembolso para o custo da renovação.

   Selecione Next (Próximo).
9. Na página Informações de contato, insira as informações de contato do registrante do domínio, dos contatos administrativos, técnicos e de cobrança. Os valores informados aqui são aplicados a todos os domínios que você está registrando. Para ter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

   Observe as seguintes considerações:

Nome e sobrenome

Para First Name e Last Name, recomendamos que você especifique o nome no seu ID oficial. Para determinadas mudanças nas configurações do domínio, alguns registros de domínio exigem que você forneça prova de identidade. O nome no documento de identificação precisa corresponder ao nome no contato do registrante para o domínio.

Contatos diferentes

Por padrão, usamos as mesmas informações para os três contatos. Se quiser inserir informações diferentes para um ou mais contatos, desmarque a caixa ao lado de Igual ao do registrante.

> **Note**
>
> Para os domínios .it, as informações de contato do registrante e do administrador devem as mesmas.

Informações necessárias adicionais

Para alguns domínios de nível superior (TLDs), é necessário coletar informações adicionais. Para esses TLDs, insira os valores aplicáveis depois do campo CEP.

Proteção da privacidade

Escolha se você deseja ocultar suas informações de contato de consultas WHOIS.

> **Note**
>
> É necessário especificar a mesma configuração de privacidade para o administrador, o registrante e os contatos técnicos.

Para obter mais informações, consulte os tópicos a seguir.

- Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio
- Domínios que você pode registrar com o Amazon Route 53

> **Note**
>
> Para habilitar a proteção de privacidade para os domínios .uk, .co.uk, .me.uk, você deve abrir um caso de suporte e solicitar proteção de privacidade.

Selecione Next (Próximo).

10. Na página Revisar, revise as informações inseridas e corrija-as se necessário. Leia os termos de serviço e marque a caixa de seleção para confirmar que você leu os termos de serviço.

    Selecione Submit request (Enviar solicitação).

11. Somente para clientes da AISPL (Índia): Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para registrar um domínio no Route 53, execute as etapas a seguir para pagar a taxa de registro do domínio.

    a. Acesse a página Pedidos e faturas no AWS Management Console.

    b. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.

    c. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

    Depois de pagar a fatura, concluímos o registro de domínio e enviamos os e-mails aplicáveis.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para registrar um domínio após o cancelamento de uma fatura, reenvie a solicitação.

Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

12. No painel de navegação, escolha Domínios e depois Solicitações.

    Nesta página, você pode ver o status do domínio e também se precisa responder ao e-mail de verificação de contato do registrante. Você também pode solicitar o reenvio do e-mail de verificação.

Se você especificou um endereço de e-mail de contato do registrante que nunca foi usado para registrar um domínio no Route 53, alguns registros TLD exigirão que você confirme que o endereço é válido.

Enviamos um e-mail de verificação de um dos seguintes endereços de e-mail:

- noreply@registrar.amazon.com: para TLDs registrados pelo Amazon Registrar.
- noreply@domainnameverification.net: para TLDs registrados por nosso associado registrador, Gandi. Para determinar quem é o registrador do seu TLD, consulte Como encontrar seu registrador.

> **Important**
>
> O contato inscrito deve seguir as instruções no e-mail para verificar se o e-mail foi recebido ou deveremos suspender o domínio conforme exigido pela ICANN. Quando um domínio é suspenso, não é possível acessá-lo na Internet.

a. Quando você receber o e-mail de verificação, escolha o link no e-mail que verifica se o endereço de e-mail é válido. Se você não receber o e-mail imediatamente, verifique sua pasta de lixo de e-mail.

b. Volte para a página Solicitações. Se o status não for atualizado automaticamente dizendo email-address is verified, escolha Refresh status.

13. Quando a transferência do domínio estiver concluída, a próxima etapa dependerá de você quer usar o Route 53 ou outro serviço DNS para o domínio:

    - Route 53: na zona hospedada que o Route 53 criou quando você registrou o domínio, crie registros para informar ao Route 53 como deseja encaminhar o tráfego para o domínio e os subdomínios.

      Por exemplo, quando alguém insere o nome de seu domínio em um navegador e essa consulta é encaminhada ao Route 53, você deseja que o Route 53 responda à consulta com o endereço IP de um servidor Web em seu datacenter ou com o nome de um balanceador de carga de Elastic Load Balancing?

      Para ter mais informações, consulte Trabalhar com registros.

> **Important**
>
> Se você criar registros em uma zona hospedada diferente daquela que o Route 53 cria automaticamente, deverá atualizar os servidores de nome do domínio para usar os servidores de nome da nova zona hospedada.

- Another DNS service (Outro serviço DNS): configure seu novo domínio para encaminhar consultas DNS para o outro serviço DNS. Execute o procedimento Atualizar servidores de nomes para usar outro registrador.

Use o procedimento a seguir para transferir até cinco domínios para sua conta.

Transferir o registro de domínio para o Route 53 para até cinco domínios

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Na página Domínios registrados, escolha Vários domínios no menu suspenso Transfência de entrada.
4. Na página Transferir vários domínios para sua conta, insira até cinco domínios que você deseja transferir e o código de autorização correspondente, se exigido, por linha e escolha Verificar.
5. Se o registro do domínio estiver disponível para transferência, ele será listado na lista Disponibilidade do domínio como disponível. Marque a caixa de seleção ao lado de cada domínio para o qual você deseja transferir o registro, verifique se cumpriu os requisitos de transferência para domínios de nível superior e escolha Avançar.

   Se o registro do domínio não estiver disponível para transferência, o console do Route 53 listará os motivos. Entre em contato com o registrador para obter informações sobre como resolver os problemas o impedem de transferir o registro.
6. Na página Serviço DNS, revise as informações sobre servidores de nomes e escolha Avançar.
7. Na página Opções de preços de domínio, escolha por quantos anos você deseja registrar o domínio para o qual você está transferindo e se deseja que renovemos automaticamente o registro do domínio antes da data de expiração.

> **Note**
>
> Os registros e as renovações de nome de domínio não são restituíveis. Se você habilitar a renovação automática do domínio e decidir que não deseja o nome de domínio depois de renovar o registro, não poderá receber reembolso para o custo da renovação.

Selecione Next (Próximo).

8. Na página Informações de contato, insira as informações de contato do registrante, do administrador e do técnico do domínio. Os valores informados aqui são aplicados a todos os domínios que você está transferindo.

> **Important**
>
> Recomendamos que você especifique os seguintes valores para o contato do registrante (o proprietário do domínio):
>
> - Nome e sobrenome: recomendamos que você especifique o nome exibido no seu ID oficial. Para determinadas mudanças nas configurações do domínio, alguns registros de domínio exigem que você forneça prova de identidade. O nome no documento de identificação precisa corresponder ao nome no contato do registrante para o domínio.
> - Detalhes de contato: durante a transferência de domínio, recomendamos que você especifique os mesmos valores especificados no registrador atual. Quando alterar os detalhes de contato para o contato do registrante, você altera o proprietário do domínio e alguns registros de TLD não permitem alterar o proprietário do domínio durante uma transferência de domínio. Se você alterar os detalhes de contato para o contato do registrante, poderá haver falha na transferência. É possível alterar os detalhes de contato para o contato do registrante depois de transferir o domínio.

Por padrão, usamos as mesmas informações para os três contatos. Se quiser inserir informações diferentes para um ou mais contatos, desmarque Igual ao contato do registrante.

> **Note**
>
> Para os domínios .it, as informações de contato do registrante e do administrador devem as mesmas.

Para ter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

9. Para alguns domínios de nível superior (TLDs), precisamos coletar informações adicionais. Para esses TLDs, insira os valores aplicáveis depois do campo CEP.
10. Se o valor de Tipo de contato for Pessoa, escolha se você deseja ocultar suas informações de contato nas consultas WHOIS. Para ter mais informações, consulte Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio.
11. Selecione Enviar.
12. Revise as informações inseridas, leia os termos de serviço e marque a caixa de seleção para confirmar que você leu os termos de serviço.
13. Selecione Submit request (Enviar solicitação).

    Nós confirmamos que o domínio é elegível para transferência e enviamos um e-mail aos contatos do registrante do domínio a fim de solicitar a autorização da transferência.
14. Somente para clientes da AISPL (Índia): Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para registrar um domínio no Route 53, execute as etapas a seguir para pagar a taxa de registro do domínio.

    a. Acesse a página Pedidos e faturas no AWS Management Console.

    b. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.

    c. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

    Depois de pagar a fatura, concluímos o registro de domínio e enviamos os e-mails aplicáveis.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para registrar um domínio após o cancelamento de uma fatura, reenvie a solicitação.

Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

15. No painel de navegação, escolha Domínios e depois Solicitações.

    Nesta página, você pode ver o status do domínio e também se precisa responder ao e-mail de verificação do contato do registrante. Você também pode solicitar o reenvio do e-mail de verificação.

    Se você especificou um endereço de e-mail de contato do registrante que nunca foi usado para registrar um domínio no Route 53, alguns registros TLD exigirão que você confirme que o endereço é válido.

    Enviamos um e-mail de verificação de um dos seguintes endereços de e-mail:

    - noreply@registrar.amazon.com: para TLDs registrados pelo Amazon Registrar.
    - noreply@domainnameverification.net: para TLDs registrados por nosso associado registrador, Gandi. Para determinar quem é o registrador do seu TLD, consulte Como encontrar seu registrador.

    > **Important**
    >
    > O contato inscrito deve seguir as instruções no e-mail para verificar se o e-mail foi recebido ou deveremos suspender o domínio conforme exigido pela ICANN. Quando um domínio é suspenso, não é possível acessá-lo na Internet.

    a. Quando você receber o e-mail de verificação, escolha o link no e-mail que verifica se o endereço de e-mail é válido. Se você não receber o e-mail imediatamente, verifique sua pasta de lixo de e-mail.

b. Volte para a página Solicitações. Se o status não for atualizado automaticamente dizendo email-address is verified, escolha Refresh status.

16. Quando a transferência do domínio estiver concluída, a próxima etapa dependerá de você quer usar o Route 53 ou outro serviço DNS para o domínio:

- Route 53: na zona hospedada que o Route 53 criou quando você registrou o domínio, crie registros para informar ao Route 53 como deseja encaminhar o tráfego para o domínio e os subdomínios.

  Por exemplo, quando alguém insere o nome de seu domínio em um navegador e essa consulta é encaminhada ao Route 53, você deseja que o Route 53 responda à consulta com o endereço IP de um servidor Web em seu datacenter ou com o nome de um balanceador de carga do ELB?

  Para ter mais informações, consulte Trabalhar com registros.

  > **Important**
  >
  > Se você criar registros em uma zona hospedada diferente daquela que o Route 53 cria automaticamente, deverá atualizar os servidores de nome do domínio para usar os servidores de nome da nova zona hospedada.

- Another DNS service (Outro serviço DNS): configure seu novo domínio para encaminhar consultas DNS para o outro serviço DNS. Execute o procedimento Atualizar servidores de nomes para usar outro registrador.

Etapa 6: apenas clientes da AISPL (Índia): pagar a taxa de transferência

Se seu endereço de contato for na Índia, seu contrato de usuário é com a Amazon Internet Services Pvt. Ltd (AISPL), uma AWS vendedora local na Índia. Para transferir um domínio para o Route 53, execute o procedimento a seguir para pagar a taxa de transferência do seu domínio.

Como pagar a taxa de transferência

1. Acesse a página Pedidos e faturas no AWS Management Console.
2. Na seção Payments Due (Pagamentos vencidos), localize a fatura aplicável.
3. Na coluna Actions (Ações), escolha Verify and Pay (Verificar e pagar).

Após o pagamento da fatura, concluímos a transferência de domínio e enviamos os e-mails aplicáveis.

> **Important**
>
> Se você não pagar a fatura em até cinco dias, ela será cancelada. Para transferir um domínio após o cancelamento de uma fatura, reenvie a solicitação.

Para obter mais informações, consulte Como gerenciar os pagamentos na Índia no Manual do usuário do AWS Billing .

Etapa 7: clicar no link nos e-mails de confirmação e autorização

Depois que você solicitar a transferência, enviaremos um ou mais e-mails para o contato registrante do domínio:

E-mail para confirmar que o contato registrante está acessível

Se você nunca registrou um domínio no Route 53 nem transferiu um domínio para o Route 53, enviaremos um e-mail solicitando que você confirme se o endereço de e-mail é válido. Nós mantemos essas informações para não precisarmos enviar este e-mail de confirmação novamente.

E-mail de autorização para transferir o domínio

Para alguns TLDs, é necessário responder a um e-mail para autorizar a transferência do domínio.

TLDs genéricos, como .com, .net e .org

A autorização não é necessária para domínios que têm um TLD genérico, como .com, .net ou .org.

TLDs geográficos, como .co.uk e .jp

Para domínios que tenham um TLD geográfico, será necessário obter a autorização para transferir o domínio. Se 10 domínios forem transferidos, teremos que enviar 10 e-mails, e você precisará clicar no link de autorização em cada um deles.

Todos os e-mails serão enviados ao contato registrante do domínio:

- Se você o contato registrante do domínio, siga as instruções do e-mail para autorizar a transferência.
- Se outra pessoa é o contato registrante do domínio, peça que essa pessoa siga as instruções do e-mail para autorizar a transferência.

> **Important**
>
> Se estiver transferindo um domínio que tenha um TLD geográfico, aguardaremos cinco dias para que o registrante entre em contato para autorizar a transferência Se o contato do registrante não responder no prazo de cinco dias, cancelaremos a operação de transferência e enviaremos um e-mail para ele informando o cancelamento.

Tópicos

E-mail de autorização para um novo proprietário ou endereço de e-mail

Se você tiver alterado os seguintes valores, nós enviaremos um e-mail separado solicitando sua autorização:

Proprietário do domínio

Se você alterar o proprietário do domínio, conforme descrito em Quem é o proprietário de um domínio?, enviaremos um e-mail para o contato do registrante do domínio.

Endereço de e-mail do contato registrante (apenas para alguns TLDs)

Para alguns TLDs, se você alterar o endereço de e-mail do contato registrante, nós enviaremos um e-mail para ambos os endereços de e-mail (antigo e novo) do contato registrante. Alguém em ambos os endereços de e-mail precisará seguir as instruções contidas no e-mail para autorizar a mudança.

No caso de alterações no proprietário do domínio ou no endereço de e-mail de contato do registrante, se não recebermos autorização para a alteração no prazo de 3 a 15 dias, dependendo do domínio de nível superior, teremos que cancelar a solicitação conforme exigido pela ICANN.

Endereços de e-mail que enviam a mensagem de autorização

Todas as mensagens são enviadas de um dos endereços de e-mail a seguir.

TLDs	Endereço de e-mail que envia a mensagem de autorização
.com.au e .net.au	no-reply@ispapi.net O e-mail contém um link para http://transfers.ispapi.net.
.fr	nic@nic.fr, se você está mudando o contato do registrante de um nome de domínio .fr ao mesmo tempo em que está transferindo o domínio. O e-mail é enviado aos contatos registrantes atual e novo.
Todos os outros	Um dos seguintes endereços de e-mail: • noreply@registrar.amazon.com • noreply@domainnameverification.net

Para determinar quem é o registrador do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

Aprovação do registrador atual

Se o contato do registrante autoriza a transferência, começamos a trabalhar com o registrador atual para transferir seu domínio. Esta etapa pode levar até dez dias, dependendo do TLD do seu domínio:

- Domínios genéricos de nível superior: leva até sete dias
- Domínios geográficos de nível superior (também conhecidos como domínios de nível superior de código de país): levam até dez dias

Se o seu registrador atual não responder nossa solicitação de transferência, fato comum entre os registradores, a transferência ocorrerá automaticamente. Se o seu registrador atual rejeitar a solicitação de transferência, enviaremos uma notificação por e-mail ao contato registrante atual. O registrante precisa entrar em contato com o registrador atual e resolver os problemas relativos à transferência.

O que acontece em seguida

Quando a transferência de domínio for aprovada, enviaremos outro e-mail para o contato do registrante. Para obter mais informações sobre o processo, consulte Visualizar o status de uma transferência de domínio.

Cobraremos sua AWS conta pela transferência do domínio assim que a transferência for concluída. Para obter uma lista de cobranças por TLD, consulte Preço do Amazon Route 53 para registro de domínio.

> **Note**
>
> Essa é uma cobrança única, então a cobrança não aparece nas suas métricas de CloudWatch faturamento. Para obter mais informações sobre CloudWatch métricas, consulte Usando CloudWatch métricas da Amazon no Guia CloudWatch do usuário da Amazon.

Etapa 8: atualizar a configuração do domínio

Depois que a transferência for concluída, você pode alterar as seguintes configurações:

Bloqueio de transferência

Para transferir o domínio para o Route 53, você precisou desabilitar o bloqueio de transferência. Se você deseja reativar o bloqueio para impedir transferências não autorizadas, consulte Bloquear um domínio para impedir uma transferência não autorizada para outro registrador.

Renovação automática

Nós configuramos o domínio transferido para renovar automaticamente à medida que a data de expiração se aproxima. Para obter informações sobre como alterar esta configuração, consulte Habilitar ou desabilitar a renovação automática de um domínio.

Período de registro estendido

Por padrão, o Route 53 renova o domínio uma vez por ano. Se você deseja registrar o domínio por um período maior, consulte Estender o período de registro de um domínio.

DNSSEC

Para obter informações sobre como configurar o DNSSEC do domínio, consulte Configurar o DNSSEC para um domínio.

Visualizar o status de uma transferência de domínio

Depois de iniciar a transferência de um domínio de outro registrador de domínio para o Amazon Route 53, você pode acompanhar o status na página Solicitações (console novo) ou Solicitações pendentes (console antigo) no console do Route 53. A coluna Status inclui uma breve descrição da etapa atual. A lista a seguir inclui o texto no console e uma descrição mais detalhada de cada etapa.

> **Note**
>
> Quando você envia uma solicitação de transferência, o status inicial é Solicitação de transferência de domínio enviada, o que indica que recebemos sua solicitação.

Determinar se o domínio atende aos requisitos de transferência (etapa 1 de 14)

Estamos confirmando que o status do seu domínio está qualificado para transferência. Você deve desbloquear seu domínio. Além disso, o domínio não pode ter qualquer um dos seguintes códigos de status quando você enviar a solicitação de transferência:

- cliente TransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

Somente TLDs geográficos: verificação de informações WHOIS (etapa 2 de 14)

Se estiver transferindo um domínio que tem um TLD geográfico, enviaremos uma consulta WHOIS para seu domínio a fim de determinar se você desativou a proteção de privacidade do domínio. Se a proteção de privacidade ainda estiver ativada com seu registrador atual, não poderemos acessar as informações de que precisamos para transferir o domínio.

> **Note**
>
> A autorização não é necessária para domínios que têm um TLD genérico, como .com, .net ou .org.

Somente TLDs geográficos: enviar e-mail ao contato inscrito a fim de obter autorização de transferência (etapa 3 de 14)

Se estiver transferindo um domínio que tem um TLD geográfico, enviaremos um e-mail ao contato do registrante do domínio. O objetivo do e-mail é confirmar se a transferência foi solicitada por um contato autorizado do domínio.

> **Note**
>
> A autorização não é necessária para domínios que têm um TLD genérico, como .com, .net ou .org.

Verificar a transferência com o registrador atual (etapa 4 de 14)

Enviamos uma solicitação ao registrador atual do domínio para iniciar a transferência.

Somente TLDs geográficos: aguardando autorização do contato inscrito (etapa 5 de 14)

Enviamos um e-mail ao contato do registrante do domínio (consulte a etapa 3 de 14) e estamos aguardando que ele clique em um link do e-mail para autorizar a transferência. Se estiver transferindo um domínio que tem um TLD geográfico e não tiver recebido esse e-mail por algum motivo, consulte Reenviar e-mails de confirmação e autorização.

Registrador atual contatado para solicitar a transferência (etapa 6 de 14)

Estamos trabalhando com o registrador atual do domínio para finalizar a transferência.

Aguardar o registrador atual para concluir a transferência (etapa 7 de 14)

Seu registrador atual está confirmando que o domínio cumpre os requisitos para ser transferido. Esta etapa pode levar até dez dias, dependendo do TLD do seu domínio:

- Domínios genéricos de nível superior: leva até sete dias
- Domínios geográficos de nível superior (também conhecidos como domínios de nível superior de código de país): levam até dez dias

> **Note**
>
> Se você aprovou o e-mail de confirmação enviado do Route 53 ao transferir um domínio .JP, mas ele parou por vários dias na ETAPA 7, entre em contato Central de Suporte da AWS para obter assistência.

Para a maioria dos registradores, o processo é totalmente automatizado e não pode ser acelerado. Alguns registradores enviam um e-mail a você solicitando que você aprove a transferência. Se o registrador enviar esse e-mail de confirmação, o processo de transferência poderá ser muito mais rápido que sete a dez dias.

Para obter informações sobre as razões que um registrador pode rejeitar a transferência, consulte Requisitos de transferência para domínios de nível superior.

Confirmar com o contato do registrante que o contato iniciou a transferência (etapa 8 de 14)

Alguns registros de TLD enviam ao contato do registrante outro e-mail para confirmar que a transferência do domínio foi solicitada por um usuário autorizado.

Sincronizar servidores de nome com o registro (etapa 9 de 14)

Esta etapa ocorre somente se os servidores de nome fornecidos como parte da solicitação de transferência são diferentes dos servidores de nome listados com o registrador atual. Tentaremos atualizar seus servidores de nome para os novos servidores de nome que você forneceu.

Sincronizar configurações com o registro (etapa 10 de 14)

Estamos verificando se a transferência foi concluída com êxito e sincronizando os dados relacionados ao domínio com o registrador associado.

Enviar informações de contato atualizadas para o registro (etapa 11 de 14)

Se você alterou a propriedade do domínio quando solicitou a transferência, estamos tentando fazer essa mudança. No entanto, a maioria dos registros não permite uma transferência de propriedade como parte do processo de transferência de domínio.

Finalizar a transferência para o Route 53 (etapa 12 de 14)

Estamos confirmando que o processo de transferência foi bem-sucedido.

Finalizar a transferência (etapa 13 de 14)

Estamos configurando seu domínio no Route 53.

Transferência completa (etapa 14 de 14)

Sua transferência foi concluída com sucesso.

Como a transferência de um domínio para o Amazon Route 53 afeta a data de validade do seu registro de domínio

Quando você transfere um domínio entre registradores, alguns registros TLD permitem que se mantenha a mesma data de expiração do domínio, outros registros acrescentam um ano à data de expiração. Há ainda os registros que alteram a data de expiração para um ano depois da data de transferência.

> **Note**
>
> Para a maioria dos TLDs, é possível estender o período de registro de um domínio por até dez anos após a sua transferência para o Amazon Route 53. Para ter mais informações, consulte Estender o período de registro de um domínio.

TLDs genéricos

Quando você transfere um domínio que tem um TLD genérico (.com, por exemplo) para o Route 53, a nova data de validade do domínio é a data de expiração que você já tinha com o registrador anterior mais um ano.

TLDs geográficos

Quando você transfere um domínio que tem um TLD geográfico (.co.uk, por exemplo) para o Route 53, a nova data de validade do domínio depende do TLD. Encontre o seu TLD na tabela a seguir para determinar como a transferência do seu domínio afeta a data de expiração.

Continente	TLDs geográficos e o efeito da transferência de um domínio na data de expiração
África	.co.za: a data de validade permanece igual.
Américas	.cl, .com.ar, .com.br: a data de validade permanece igual.

Continente	TLDs geográficos e o efeito da transferência de um domínio na data de expiração
	.ca, .co, .mx, .us: um ano é adicionado à data de validade antiga.
Ásia/Oceania	.co.nz, .com.au, .com.sg, .jp, .net.au, .net.nz, .org.nz, .sg: a data de validade permanece igual. .in: um ano é adicionado à data de validade antiga.
Europa	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se: a data de validade permanece igual. .berlin, .eu, .io, .me, .ruhr, .wien: um ano é adicionado à data de validade antiga. .be, .de, .fr, .it, .nl: a nova data de validade é um ano depois da data da transferência.

Transferir um domínio para uma conta diferente AWS

Se você registrou um domínio usando uma AWS conta e quiser transferir o domínio para outra AWS conta, poderá transferi-lo facilmente usando o novo console ou usando o AWS CLI ou outros métodos programáticos.

Tópicos

Etapa 1: transferir um domínio para uma AWS conta diferente

Os domínios não podem ser transferidos nos primeiros 14 dias após o registro.

Ao iniciar a transferência de um domínio, é necessário fazer login usando a conta raiz ou usando um usuário que tenha recebido permissões do IAM de uma das seguintes maneiras:

- A política AdministratorAccessgerenciada é atribuída ao usuário.

- O usuário recebe a política gerenciada AmazonRoute53 DomainsFull Access.
- O usuário recebe a política FullAccess gerenciada AmazonRoute53.
- O usuário recebe a política gerenciada de PowerUseracesso.
- O usuário tem permissão para realizar todas as ações a seguir: `TransferDomains`, `DisableDomainTransferLock` e `RetrieveDomainAuthCode`.

Se você não fizer login usando a conta raiz ou um usuário do que tenha as permissões necessárias, não poderemos fazer a transferência. Esse requisito impede que usuários não autorizados transfiram domínios para outros. Contas da AWS

O processo de transferência tem duas etapas. Primeiro, o proprietário da conta de origem inicia a transferência: no procedimento de iniciar uma transferência para outra Conta da AWS e depois o proprietário da conta de destino aceita a transferência no procedimento de aceitar uma transferência de outra Conta da AWS.

Para transferir um domínio para uma AWS conta diferente

1. Faça login AWS usando o domínio no Conta da AWS qual o domínio está registrado no momento.
2. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Domínios registrados.
4. Escolha o nome do domínio que você deseja transferir para outra Conta da AWS.
5. Acima da seção Detalhes, no menu suspenso Transfência de saída, escolha Transferir para outra Conta da AWS.
6. Na caixa de diálogo Transferir para outra Conta da AWS, insira o ID da conta de destino. Você pode obter esse ID com o proprietário da Conta da AWS de destino.
7. Selecione a opção Confirmar.
8. Na caixa de diálogo Gerar senha, copie a senha e encaminhe-a para o Conta da AWS proprietário destinatário.

   Na página Solicitações, o Status do domínio será Em andamento e o Tipo será Transferência interna de saída.

Para aceitar uma transferência de domínio de uma AWS conta diferente

1. Faça login AWS usando o Conta da AWS que está recebendo o domínio.

2. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, selecione Solicitações.
4. Na página Solicitações, selecione o botão de rádio ao lado do nome de domínio que você está transferindo de outro Conta da AWS. Se o domínio estiver pronto para ser transferido, o status será Ação necessária e o Tipo será Transferência interna de entrada de domínio.

   Você tem três dias para aceitar a solicitação. Se essa transferência não for aceita em três dias, ela será cancelada.
5. No menu suspenso Ação, escolha Aceitar.

   Você também pode escolher Rejeitar para cancelar o processo de transferência.
6. Se você aceitou, na página Transferir domínio para sua conta, na seção Senha, insira a senha que recebeu do proprietário da conta de origem.

   Aceite os termos e condições, e escolha Avançar.
7. Navegue até a página Solicitações para monitorar o status da transferência e as outras etapas a serem concluídas.
8. Depois que a transferência for concluída, você poderá atualizar as informações de contato. Para ter mais informações, consulte Atualizar informações de contato e propriedade de um domínio.

Transferir o domínio programaticamente

Você também pode transferir o domínio programaticamente usando um dos AWS SDKs ou a API do Route 53. AWS CLI Para obter mais informações, consulte a seguinte documentação do :

- Para obter uma visão geral do processo de transferência e a documentação sobre as ações de API que você usa para transferir um domínio usando a API de registro de domínio do Route 53, consulte TransferDomainToAnotherAwsAccounta Referência de API do Amazon Route 53.
- Para obter documentação sobre outras opções para transferir domínios programaticamente, consulte “SDKs e kits de ferramentas” na seção Guias e referências de API da página “documentação”.AWS
- A conta destinatária tem três dias para aceitar a transferência da conta de origem, usando a API transfer-domain-to-another-aws-account. Se essa transferência não for aceita em três dias, ela será cancelada.

> **Important**
>
> Quando você transfere um domínio para uma AWS conta diferente programaticamente, a zona hospedada do domínio não é transferida. Se você desejar transferir a zona hospedada também, aguarde até que o domínio tenha sido transferido e consulte Etapa 2 (opcional): migrar uma zona hospedada para uma conta diferente AWS.

Etapa 2 (opcional): migrar uma zona hospedada para uma conta diferente AWS

Se você estiver usando o Route 53 como o serviço DNS do domínio, o Route 53 não transferirá a zona hospedada quando você transferir um domínio para outra conta da AWS . Se o registro de domínio está associado a uma conta e a zona hospedada correspondente está associada a outra conta, nem o registro de domínio nem a funcionalidade do DNS são afetados. A única consequência é que você precisará fazer login no console do Route 53 usando uma conta para ver o domínio e fazer login usando a outra conta para ver a zona hospedada.

Se você for o proprietário da conta da qual está transferindo o domínio e da conta à qual está transferindo o domínio, você pode migrar a zona hospedada do domínio para outra conta, mas isso não é obrigatório. O Route 53 continuará usando os registros na zona hospedada existente para encaminhar o tráfego para o domínio.

> **Important**
>
> Se você não possui a conta da qual está transferindo o domínio e a conta para a qual está transferindo o domínio, você deve migrar a zona hospedada existente para a AWS conta para a qual você está transferindo o domínio ou criar uma nova zona hospedada em uma AWS conta de sua propriedade. Se você não é o proprietário da conta que criou a zona hospedada que roteia o tráfego para o domínio, não pode controlar como o tráfego é roteado.

Para migrar a zona hospedada existente para a nova conta, consulte Migrando uma zona hospedada para uma conta diferente AWS.

Para criar uma nova zona hospedada, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente. Esse tópico geralmente é usado quando você transfere domínios de outro registrador para o Route 53, mas o processo é o mesmo quando você transfere domínios de uma conta para outra AWS .

Como transferir um domínio do Amazon Route 53 para outro registrador

Quando você transfere um domínio do Amazon Route 53 para outro registrador, você obtém algumas informações do Route 53 e fornece-as ao novo registrador. O novo registrador fará o restante.

> **Important**
>
> Se você estiver usando o Route 53 como seu provedor de serviço DNS e quiser transferir o serviço DNS também para outro provedor, lembre-se de que os recursos do Route 53 a seguir não têm equivalentes diretos nos recursos fornecidos por outros provedores de serviço DNS. Você precisará trabalhar com o novo provedor de serviço de DNS para determinar como alcançar uma funcionalidade comparável:
>
> - Registros de alias. Para ter mais informações, consulte Escolher entre registros de alias e não alias.
> - Roteamento de políticas diferentes da política de roteamento simples. Para ter mais informações, consulte Escolher uma política de roteamento.
> - Verificações de integridade associadas com registros. Para ter mais informações, consulte Configurar failover de DNS.

A maioria dos registradores de domínio impõe requisitos sobre a transferência de um domínio para outro registrador. O objetivo principal desses requisitos é impedir que os proprietários de domínios fraudulentos transfiram repetidamente os domínios para diferentes registradores. Os requisitos variam, mas os seguintes requisitos são típicos:

- Você deve ter registrado o domínio com o registrador atual ou transferido o registro do domínio para o registrador atual há pelo menos 60 dias.
- Se o registro de um nome de domínio expirou e precisou ser restaurado, ele deve ter sido restaurado há pelo menos 60 dias.
- O domínio não pode ter qualquer um dos seguintes códigos de status de nome de domínio:
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - cliente TransferProhibited

Para ver uma lista atualizada de códigos de status de nomes de domínio e uma explicação do que cada código significa, acesse o site da ICANN e procure os códigos de status EPP. (Pesquise no site da ICANN; às vezes as pesquisas da Web retornam uma versão antiga do documento.)

> **Note**
>
> Se você quiser transferir seu domínio para outro registrador de domínio, mas a AWS conta na qual o domínio está registrado estiver fechada, suspensa ou encerrada, entre em contato com o AWS Support para obter ajuda. Os domínios não podem ser transferidos nos primeiros 14 dias após o registro. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

> **Note**
>
> Se o novo registrador exigir um código REG-ID, você pode entrar em contato com o AWS Support para obter ajuda. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Para transferir um domínio do Route 53 para outro registrador

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio que você deseja transferir para outro registrador.
4. Na página Domínios registrados, verifique o valor do Código de status do nome do domínio. Se o status for um dos valores a seguir, você não poderá transferir o domínio neste momento:
   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - cliente TransferProhibited
   - servidor TransferProhibited

Para ver uma lista atualizada de códigos de status de nomes de domínio e uma explicação do que cada código significa, acesse o site da ICANN e procure os códigos de status EPP. (Pesquise no site da ICANN; às vezes as pesquisas da Web retornam uma versão antiga do documento.)

Se o valor do código de status do nome de domínio for servidor TransferProhibited, você poderá entrar em contato com o AWS Support gratuitamente para saber o que fazer para poder transferir o domínio. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

5. Se o valor de Bloqueio de transferência for Ativado, escolha Desativar bloqueio de transferência no menu suspenso Ações.

> **Note**
>
> Entre em contato com o AWS Support para desbloquear a transferência de domínios.jp pelo registrador. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

6. Todos os domínios, exceto os domínios.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk e .org.uk — Na página do nome de domínio, escolha Transferir para outro registrador no menu suspenso Transferir para fora.

   Na caixa de diálogo Transferir para outro registrador, escolha Copiar para copiar o código de autorização da transferência de domínio. Você vai fornecer esse valor para o seu registrador mais adiante neste procedimento.

   Domínios.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk e .org.uk — Faça o seguinte:

   domínios.be

   Obtenha o código de autorização do registro de domínios.be no site da DNS Belgium.

   Domínios .co.za

   Não é necessário obter um código de autorização para transferir um domínio .co.za a outro registrador.

Domínios .es

Não é necessário obter um código de autorização para transferir um domínio .es para outro registrador.

domínios .ru

Obtenha o código de autorização do registro para domínios .ru em https://www.nic.ru/en/auth/recovery/:

a. Selecione a opção para recuperar credenciais por nome de domínio.
b. Insira o nome de domínio e selecione Continue (Continuar).
c. Siga as instruções na tela para obter acesso à página de admin RU-CENTER.
d. Na seção Manage your account (Gerenciar sua conta), selecione Domain transfer (Transferência de domínio).
e. Confirme a transferência com REGRU-RU.

domínios .uk, .co.uk, .me.uk e .org.uk

Altere a tag de IPS para o valor do novo registrador:

a. Acesse a página Find a Registrar no site da Nominet e localize a tag de IPS do novo registrador. (Nominet é o órgão responsável pela gestão dos domínios .uk, co.uk, .me.uk e .org.uk.)
b. Na página Registered Domains> (Domínios registrados) domain name (nome do domínio), em IPS Tag (Etiqueta IPS), escolha Change IPS Tag (Alterar etiqueta IPS) e especifique o valor obtido na etapa 7a.
c. Selecione Atualizar.

7. Se, no momento, você não estiver usando o Route 53 como o provedor de serviços DNS do seu domínio, vá para a etapa 10.

   Se você estiver usando o Route 53 como o provedor de serviço DNS do domínio, execute as seguintes etapas:

   a. Selecione Hosted Zones (Zonas hospedadas).
   b. Escolha o nome da zona hospedada para seu domínio. O domínio e a zona hospedada têm o mesmo nome.
   c. Se quiser continuar usando o Route 53 como o provedor de serviço DNS do domínio: obtenha os nomes dos quatro servidores de nome que o Route 53 atribuiu à sua zona

hospedada. Para ter mais informações, consulte Obter os servidores de nome de uma zona hospedada pública.

Se não quiser continuar usando o Route 53 como o provedor de serviço DNS do domínio: anote as configurações de todos os seus registros, exceto os registros SOA e NS. Para os recursos específicos do Route 53, como registros de alias, você precisará trabalhar com seu novo provedor de serviço DNS para determinar como alcançar uma funcionalidade comparável.

8. Se você está transferindo o serviço de DNS para outro provedor, use os métodos fornecidos pelo novo serviço de DNS para executar as seguintes tarefas:

   - Criar uma zona hospedada
   - Criar registros que reproduzem a funcionalidade de seus registros do Route 53
   - Obtenha os servidores de nome que o novo serviço de DNS atribuiu à sua zona hospedada

9. Solicite uma transferência do domínio adotando o processo fornecido pelo novo registrador.

   Todos os domínios, exceto os domínios.co.za, .es, .uk, .co.uk, .me.uk e .org.uk — você será solicitado a inserir o código de autorização obtido do console do Route 53 na etapa 6 deste procedimento.

10. Se você ainda quiser usar o Route 53 como seu provedor de serviços DNS, use o processo fornecido pelo novo registrador para especificar os nomes dos servidores de nomes do Route 53 que você obteve na etapa 7. Se você quiser usar outro provedor de serviços DNS, especifique os nomes dos servidores de nomes que o novo provedor forneceu quando você criou uma nova zona hospedada na etapa 8.

11. Responda ao e-mail de confirmação:

    Todos os domínios, exceto domínios .jp

    O Route 53 envia um e-mail de confirmação para o endereço de e-mail do contato do registrante para o domínio:

    - Se você não responder ao e-mail, a transferência ocorrerá automaticamente na data especificada.
    - Se você quiser que a transferência ocorra antes, ou quiser cancelar a transferência, escolha o link no e-mail para acessar o site do Route 53 e escolha a opção apropriada.
    - Dependendo do TLD, o e-mail de confirmação poderá conter um link para https://approvemove.com, onde você pode aprovar ou rejeitar a transferência. Quando a proteção

de privacidade estiver ativada para os contatos do domínio, o e-mail será entregue pelos endereços identity-protect.org para TLDs registrados no Amazon Registrar. Para determinar quem é o registrador do seu TLD, consulte Como encontrar seu registrador.

domínios .jp

O Route 53 envia um e-mail de confirmação para o endereço de e-mail do contato do registrante do domínio do endereço noreply@domainnameverification.net com um link para confirmar a transferência:

- Se você não responder ao e-mail, a transferência será cancelada na data especificada.
- Se você quiser que a transferência ocorra antes, ou quiser cancelar a transferência, escolha o link no e-mail para acessar o site do Route 53 e escolha a opção apropriada. Você terá que fornecer o código de autorização de domínio obtido na etapa 7.

Além disso, você pode receber um e-mail de WIXI.jp. Você pode ignorar esse erro.

12. Se o registrador para o qual você está transferindo o domínio relatar que a transferência falhou, entre em contato com o registrador para obter mais informações. Quando você transfere um domínio para outro registrador, todas as atualizações de status vão para o novo registrador, portanto, o Route 53 não tem informações sobre o motivo de falha de uma transferência.

    Se o novo registrador informar que a transferência falhou porque o código de autorização que você recebeu do Route 53 não é válido, abra um caso com o AWS Support. (Você não precisa de um contrato de suporte, e não há taxas.) Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

13. Se você transferiu o serviço DNS para outro provedor de serviços DNS, você pode excluir os registros da zona hospedada e a própria zona hospedada depois que os resolvedores de DNS pararem de responder às consultas de DNS com os nomes dos servidores de nomes do Route 53. Isso geralmente leva dois dias, ou seja, o tempo durante o qual os resolvedores de DNS normalmente armazenam os nomes dos servidores de nomes em cache para um domínio.

    > **Important**
    >
    > Se você excluir a zona hospedada enquanto os resolvedores de DNS ainda estiverem respondendo a consultas de DNS com os nomes dos servidores de nomes do Route 53, seu domínio ficará indisponível na Internet.

Depois de excluir a zona hospedada, o Route 53 interromperá o faturamento da taxa mensal de uma zona hospedada. Para obter mais informações, consulte a seguinte documentação do :

- Excluir registros
- Excluir uma zona hospedada pública
- Preço do Route 53

Transferência do registrador para o Amazon Registrar

O Amazon Route 53 Domains usa dois registradores para registrar domínios para clientes: Amazon Registrar, um registrador de propriedade e operado por AWS, e Gandi, um registrador associado com quem trabalhamos. Inicialmente, a maioria dos domínios do Route 53 foram registrados por meio de Gandi porque o Amazon Registrar não era diretamente credenciado para muitos domínios de primeiro nível (TLDs), como .com ou .club. Agora que o Amazon Registrar está diretamente credenciado com centenas de TLDs (e crescendo), começaremos a transferir domínios registrados por meio do Gandi para o Amazon Registrar em seu nome.

Isso não mudará a forma como você gerencia o domínio no Route 53, apenas atualizará o registrador de registro do seu domínio de Gandi para o Amazon Registrar. A transferência ocorrerá durante o processo de renovação do domínio e somente a taxa de renovação padrão será aplicada. Depois que a transferência for concluída, novas solicitações para transferir seu domínio para um novo registrador externo AWS poderão ser adiadas. O Route 53 informará os registrantes de domínio afetados 15 dias antes da transferência na renovação. Esse processo é descrito em nosso Contrato de Registro de Nomes de Domínio (consulte a seção 3.11.5).

Essa transferência é obrigatória se você quiser continuar usando o serviço Route 53 para gerenciar seus domínios. Se você não quiser usar o Amazon Registrar para gerenciar seu domínio, você precisará transferir seu domínio para outro registrador dentro de 15 dias após receber o aviso de transferência na renovação do AWS.

Reenviar e-mails de confirmação e autorização

Para várias operações relacionadas ao registro de domínios, a ICANN exige que obtenhamos autorização do contato registrante do domínio ou a confirmação de que o endereço de e-mail do contato registrante é válido. Para obter a autorização ou a confirmação, enviamos a você um e-mail

que contém um link. Você tem entre 3 e 15 dias para clicar no link, dependendo da operação e do domínio de nível superior. Depois desse período, o link deixa de funcionar.

Geralmente, quando você não clica no link contido no e-mail dentro do prazo atribuído, a ICANN exige a suspensão do domínio ou o cancelamento da operação, dependendo da ação que você estava tentando realizar:

Registrar um domínio

Nós suspendemos o domínio. Dessa forma, não é possível acessá-lo na Internet. Para reenviar o e-mail de confirmação, consulte Para reenviar o e-mail de confirmação de um registro de domínio.

Somente TLDs geográficos: transferir um domínio para o Amazon Route 53

Se estiver transferindo um domínio que tem um TLD geográfico, cancelaremos a transferência. Para reenviar o e-mail de autorização, consulte Para reenviar o e-mail de autorização para transferência de um domínio.

> **Note**
>
> A autorização não é necessária para domínios que têm um TLD genérico, como .com, .net ou .org.

Alterar o nome ou o endereço de e-mail do contato registrante do domínio (o proprietário)

Nós cancelamos a alteração. Para reenviar o e-mail de autorização, consulte Para reenviar o e-mail de autorização e atualizar o contato registrante ou excluir um domínio.

Excluir um domínio

Nós cancelamos a solicitação de exclusão. Para reenviar o e-mail de autorização, consulte Para reenviar o e-mail de autorização e atualizar o contato registrante ou excluir um domínio.

Somente TLDs geográficos: transferir um domínio do Route 53 para outro registrador

Se estiver transferindo um domínio que tenha um TLD geográfico, o novo registrador cancelará a transferência.

> **Note**
>
> A autorização não é necessária para domínios que têm um TLD genérico, como .com, .net ou .org.

Tópicos

Atualizar seu endereço de e-mail

Sempre enviamos e-mails de confirmação e autorização para o endereço de e-mail do contato registrante de um domínio. Para alguns TLDs, somos obrigados a enviar o e-mail para ambos os endereços de e-mail (antigo e novo) do contato registrante nos seguintes casos:

- Se você estiver alterando o endereço de e-mail de um domínio já registrado no Amazon Route 53
- Se você estiver alterando o endereço de e-mail de um domínio que você está transferindo para o Route 53

Reenviar e-mails

Use o procedimento aplicável para reenviar e-mails de autorização ou confirmação.

- Para reenviar o e-mail de confirmação de um registro de domínio
- Para reenviar o e-mail de autorização para transferência de um domínio
- Para reenviar o e-mail de autorização e atualizar o contato registrante ou excluir um domínio

Para reenviar o e-mail de confirmação de um registro de domínio

1. Verifique o endereço de e-mail do contato registrante e, se necessário, atualize-o. Para ter mais informações, consulte Atualizar informações de contato e propriedade de um domínio.
2. Verifique a pasta de spam no seu aplicativo de e-mail para ver há e-mails de um dos seguintes endereços de e-mail.

Se o e-mail foi enviado há muito tempo, o link não funcionará mais. No entanto, você saberá onde localizar o e-mail de confirmação quando o enviarmos novamente.

TLDs	Endereço de e-mail que envia o e-mail de aprovação ou confirmação
.fr	nic@nic.fr
Todos os outros	Um dos seguintes endereços de e-mail: • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **Note**
>
> Os e-mails podem conter um link para www.verify-whois.com. É seguro usar esse link.

3. Use o console do Amazon Route 53 para reenviar o e-mail de confirmação:

   a. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   b. No painel de navegação, escolha Domínios registrados.

   c. Escolha o nome do domínio para o qual você deseja reenviar o e-mail.

   d. Na caixa de aviso com cabeçalho "Seu domínio pode ser suspenso", escolha a opção Enviar e-mail novamente.

   > **Note**
   >
   > Se não houver nenhuma caixa de aviso, significa que você já confirmou que o endereço de e-mail do contato registrante é válido.

4. Se você tiver problemas ao reenviar o e-mail de confirmação, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Para reenviar o e-mail de autorização para transferência de um domínio

Esse método não funciona para solicitações de transferência de domínio .jp.

1. Use o método fornecido pelo registrador de domínio atual para confirmar que a proteção de privacidade do domínio está desativada. Se não estiver, desative-a.

   Nós enviamos o e-mail de autorização para o endereço de e-mail que o registrador atual salvou no banco de dados WHOIS. Geralmente, quando a proteção de privacidade está ativada, esse endereço de e-mail não pode ser lido. O registrador atual pode não encaminhar ao seu endereço de e-mail atual o e-mail que o Amazon Route 53 envia para o endereço de e-mail contido no banco de dados WHOIS.

   > **Note**
   >
   > Se o registrador atual do domínio não permitir a desativação da proteção de privacidade, ainda poderemos transferir o domínio se você tiver especificado um código de autorização válido em Etapa 5: solicitar a transferência.

2. Verifique o endereço de e-mail do contato registrante e, se necessário, atualize-o. Use o método fornecido pelo registrador atual do domínio.
3. Verifique a pasta de spam no seu aplicativo de e-mail para ver há e-mails de um dos seguintes endereços de e-mail.

   Se o e-mail foi enviado há muito tempo, o link não funcionará mais. No entanto, você saberá onde localizar o e-mail de autorização quando o enviarmos novamente.

TLDs	Endereço de e-mail que envia o e-mail de aprovação ou confirmação
.com.au e .net.au	no-reply@ispapi.net O e-mail contém um link para https://approve.domainadmin.com.
.fr	nic@nic.fr
Todos os outros	Um dos seguintes endereços de e-mail:

TLDs	Endereço de e-mail que envia o e-mail de aprovação ou confirmação
	• noreply@registrar.amazon.com • noreply@domainnameverification.net

> **Note**
>
> Os e-mails podem conter um link para www.verify-whois.com. É seguro usar esse link.

4. Se a transferência não estiver mais sendo processada (em caso de cancelamento devido ao prazo fornecido), solicite-a novamente para que possamos enviar para você outro e-mail de autorização.

> **Note**
>
> Nos primeiros 15 dias após a solicitação da transferência, você poderá determinar o status da transferência verificando a tabela Notifications (Notificações) na página Dashboard (Painel) do console do Route 53. Depois de 15 dias, use o AWS CLI para obter o status. Para obter mais informações, consulte route53domains na Referência de comando da AWS CLI .

Se a transferência ainda estiver em andamento, siga estas etapas para reenviar o e-mail de autorização.

a. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
b. Na tabela Notifications (Notificações), localize o domínio que você deseja transferir.
c. Na coluna Status desse domínio, escolha Reenviar e-mail.

5. Se você tiver problemas ao reenviar o e-mail de autorização para uma transferência de domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Para reenviar o e-mail de autorização e atualizar o contato registrante ou excluir um domínio

1. Verifique o endereço de e-mail do contato registrante e, se necessário, atualize-o. Para ter mais informações, consulte Atualizar informações de contato e propriedade de um domínio.
2. Verifique a pasta de spam no seu aplicativo de e-mail para ver há e-mails de um dos seguintes endereços de e-mail.

   Se o e-mail foi enviado há muito tempo, o link não funcionará mais. No entanto, você saberá onde localizar o e-mail de autorização quando o enviarmos novamente.

TLDs	Endereço de e-mail que envia o e-mail de autorização
.fr	nic@nic.fr
Todos os outros	Um dos seguintes endereços de e-mail: • noreply@registrar.amazon.com • noreply@domainnameverification.net

> **Note**
>
> Os e-mails podem conter um link para www.verify-whois.com. É seguro usar esse link.

3. Cancele a alteração ou exclusão. Você tem duas opções:

   - Você pode aguardar o período de espera de 3 a 15 dias. Depois desse período, cancelamos automaticamente a operação solicitada.
   - Como alternativa, você pode entrar em contato com o AWS Support e pedir que eles cancelem a operação.
4. Depois que a alteração ou exclusão for cancelada, você poderá alterar as informações de contato ou excluir o domínio novamente, e nós enviaremos outro e-mail de autorização.
5. Se você tiver problemas ao reenviar o e-mail de autorização, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Configurar o DNSSEC para um domínio

Às vezes, invasores sequestram o tráfego para endpoints da Internet, como servidores da Web, interceptando consultas de DNS e retornando seus próprios endereços IP para os resolvedores de DNS no lugar dos endereços IP reais desses endpoints. Então, os usuários são direcionados para os endereços IP fornecidos pelo invasores na resposta falsificada, por exemplo, para sites falsos.

Você pode proteger seu domínio contra esse tipo de ataque, conhecido como falsificação de DNS ou man-in-the-middle ataque, configurando as Extensões de Segurança do Sistema de Nomes de Domínio (DNSSEC), um protocolo para proteger o tráfego DNS.

> **Important**
>
> O Amazon Route 53 é compatível com assinatura de DNSSEC e DNSSEC para registro de domínio. Se você quiser configurar a assinatura de DNSSEC para um domínio que está registrado com o Route 53, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

Tópicos

Visão geral de como o DNSSEC protege o seu domínio

Quando você configura o DNSSEC para o seu domínio, um resolvedor de DNS estabelece uma cadeia de confiança para respostas de resolvedores intermediários. A cadeia de confiança começa com o registro do TLD do domínio (a zona principal do domínio) e termina com os servidores de nome autorizados no seu provedor de serviços de DNS. Nem todos os resolvedores de DNS oferecem suporte ao DNSSEC. Apenas os resolvers compatíveis com DNSSEC realizam assinatura ou validação de autenticidade.

Veja, de maneira simplificada, como configurar o DNSSEC para domínios registrados no Amazon Route 53 para proteger seus hosts de Internet contra falsificação de DNS:

1. Use o método fornecido pelo seu provedor de serviços de DNS para assinar os registros em sua zona hospedada com a chave privada em um par de chaves assimétricas.

   > **Important**
   >
   > O Route 53 é compatível com assinatura de DNSSEC e DNSSEC para registro de domínio. Para saber mais, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

2. Forneça a chave pública do par de chaves ao registrador do domínio e especifique o algoritmo que foi usado para gerar o par de chaves. O registrador do domínio encaminhará a chave pública e o algoritmo do registro para o domínio de nível superior (TLD).

   Para obter informações sobre como executar essa etapa para os domínios que você registrou no Route 53, consulte Adicionar chaves públicas a um domínio.

Depois de configurar o DNSSEC, veja como ele protege seu domínio contra falsificação de DNS:

1. Para enviar uma consulta de DNS, por exemplo, navegue até um site ou envie uma mensagem de e-mail.
2. A solicitação é encaminhada para um resolvedor de DNS. Os resolvedores são responsáveis por retornar o valor apropriado para os clientes com base na solicitação, por exemplo, o endereço IP do host que está executando um servidor da Web ou de e-mail.
3. Se o endereço IP for armazenado em cache no resolver de DNS porque alguém já enviou a mesma consulta ao DNS e o resolver já obteve o valor, o resolver retornará o endereço IP para o cliente que enviou a solicitação. Então, o cliente usa o endereço IP para acessar o host.

   Se o endereço IP não estiver armazenado em cache no resolvedor de DNS, o resolvedor enviará uma solicitação à zona principal do seu domínio, no registro do TLD, que retornará dois valores:

   - O registro do Signatário de Delegação (DS), que é uma chave pública correspondente à chave privada usada para assinar o registro.
   - Os endereços IP de servidores de nome autorizados para o seu domínio.
4. O resolvedor de DNS envia a solicitação original para outro resolvedor de DNS. Se esse resolvedor não tiver o endereço IP, ele repetirá o processo até que um resolvedor envie a solicitação para um servidor de nome no seu provedor de serviços de DNS. O servidor de nome retorna dois valores:

- O registro do domínio, como example.com. Normalmente, ele contém o endereço IP de um host.
- A assinatura do registro, que você criou quando configurou o DNSSEC.

5. O resolver de DNS usa a chave pública que você forneceu ao registrador de domínio e que o registrador encaminhou para o registro de TLD com duas finalidades:
   - Estabelecer uma cadeia de confiança.
   - Verificar se a resposta assinada do provedor de serviços de DNS é legítima e não foi substituída por uma resposta inválida de um invasor.
6. Se a resposta for autêntica, o resolvedor retornará o valor para o cliente que enviou a solicitação.

   Se a resposta não puder ser verificada, o resolvedor retornará um erro para o usuário.

   Se o registro de TLD do domínio não tiver a chave pública para o domínio, o resolvedor responderá à consulta de DNS usando a resposta recebida do provedor de serviços de DNS.

Pré-requisitos e máximos para configurar o DNSSEC para um domínio

Para configurar o DNSSEC em um domínio, o provedor de serviços de DNS e o domínio devem atender aos seguintes pré-requisitos:

- O registro do TLD deve oferecer suporte ao DNSSEC. Para determinar se o registro do seu TLD oferece suporte ao DNSSEC, consulte Domínios que você pode registrar com o Amazon Route 53.
- O provedor de serviços de DNS do domínio deve oferecer suporte ao DNSSEC.

> **Important**
>
> O Route 53 é compatível com assinatura de DNSSEC e DNSSEC para registro de domínio. Para saber mais, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

- Você deve configurar o DNSSEC com o provedor de serviços de DNS do seu domínio antes de adicionar chaves públicas do domínio ao Route 53.
- O número de chaves públicas que você pode adicionar a um domínio depende do TLD dele:
  - Domínios .com e .net: até 13 chaves
  - Todos os outros domínios: até quatro chaves

Adicionar chaves públicas a um domínio

Quando você fizer a mudança de chaves ou a ativação do DNSSEC para um domínio, execute o procedimento a seguir, depois de configurar o DNSSEC com o provedor de serviços de DNS do domínio.

Para adicionar chaves públicas a um domínio

1. Se você ainda não configurou o DNSSEC com seu provedor de serviços de DNS, use o método fornecido pelo seu provedor de serviço para configurá-lo.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Domínios registrados.
4. Escolha o nome do domínio ao qual você deseja adicionar chaves.
5. Escolha a guia Chave do DNSSEC escolha Adicionar chave.
6. Especifique os seguintes valores:

   Tipo de chave

   Escolha se você deseja fazer upload de uma chave de assinatura de chaves (KSK) ou de uma chave de assinatura de zonas (ZSK).

   Algoritmo

   Escolha o algoritmo que você usou para assinar os registros da zona hospedada.

   Chave pública

   Especifique a chave pública do par de chaves assimétricas que você usou para configurar o DNSSEC com seu provedor de serviços de DNS.

   Observe o seguinte:

   - Especifique a chave pública, não o resumo.
   - É necessário especificar a chave no formato base64.
7. Escolha Adicionar.

> **Note**
>
> Você pode adicionar apenas uma chave pública por vez. Se você precisar adicionar mais chaves, aguarde até receber um e-mail de confirmação do Route 53.

8. Quando o Route 53 recebe uma resposta do registro, nós enviamos um e-mail para o contato registrante do domínio. O e-mail confirma que a chave pública foi adicionada ao domínio no registro ou explica por que não foi possível adicioná-la.

Excluir chaves públicas de um domínio

Quando você fizer a mudança de chaves ou a desativação do DNSSEC para o domínio, exclua as chaves públicas utilizando o procedimento a seguir, antes de desativar o DNSSEC com o provedor de serviços de DNS. Observe o seguinte:

- Ao fazer a mudança das chaves públicas, recomendamos que você aguarde até três dias depois de adicionar as novas chaves públicas para excluir as antigas.
- Ao desativar o DNSSEC, primeiro exclua as chaves públicas do domínio. Recomendamos que você aguarde até três dias antes de desativar o DNSSEC com o serviço DNS do domínio.

> **Important**
>
> Se o DNSSEC estiver ativado para o domínio e você desativar esse protocolo com o serviço DNS, os resolvedores de DNS que oferecem suporte a ele retornarão um erro `SERVFAIL` para os clientes, que não poderão acessar os endpoints associados ao domínio.

Para excluir chaves públicas de um domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio do qual você deseja excluir chaves.
4. Na guia Chaves do DNSSEC, selecione o botão de opção ao lado da chave que você deseja excluir e depois selecione Excluir chave.

5. Na caixa de diálogo Excluir chave do DNSSEC, insira excluir na caixa de texto para confirmar que deseja excluir a chave e escolha Excluir.

> **Note**
>
> Você pode excluir apenas uma chave pública por vez. Se precisar excluir mais chaves, aguarde até receber um e-mail de confirmação do Amazon Route 53.

6. Quando o Route 53 recebe uma resposta do registro, nós enviamos um e-mail para o contato registrante do domínio. O e-mail confirma que a chave pública foi excluída do domínio no registro ou explica por que não foi possível excluí-la.

Como encontrar seu registrador e outras informações sobre seu domínio

Para visualizar as informações do domínio usando a API GetDomainDetail, você pode usar qualquer um dos SDKs ou AWS CLI. Para obter mais informações, consulte get-domain-detail.

Para visualizar informações sobre domínios com CLI **`get-domain-detail`**

- Use o seguinte CLI:

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> Esse comando só é executado em us-east-1 Região da AWS.

Todas as informações sobre seu domínio serão listadas na saída, incluindo o registrador, a data de registro, a configuração de privacidade etc.

Visualizar informações sobre domínios registrados no Route 53

É possível visualizar informações sobre os domínios registrados usando o Route 53. Essas informações incluem detalhes como quando o domínio foi originalmente registrado e informações de contato do proprietário do domínio e dos contatos técnicos, administrativos e de cobrança.

WHOIS

WHOIS é um diretório gratuito e disponível ao público que contém informações sobre domínios patrocinados por registradores e registros de domínios. Ele é fornecido como um serviço que aceita consultas na porta 43 e como um site, cada um acessível via IPv4 e IPv6. O WHOIS é uma pesquisa hierárquica distribuída. Para obter mais informações, consulte Sobre o WHOIS.

Uma solicitação ao WHOIS em diferentes níveis da hierarquia pode fornecer informações diferentes:

- Uma solicitação ao WHOIS raiz (whois.iana.org) fornece informações sobre o registro.
- Uma solicitação ao registro do WHOIS fornece informações sobre o registrador e algumas informações públicas sobre o domínio.
- Uma solicitação ao registrador do WHOIS fornece todas as informações públicas sobre o domínio.

Como o WHOIS tem vários níveis, incluindo pesquisas de WHOIS operadas pelo registro de TLD e pelo registrador de domínios, desativar sua proteção de privacidade no console do Route 53 só pode desativá-la no WHOIS fornecido pelo registrador. Alguns registros mantêm intencionalmente serviços de proteção de privacidade ou ocultação para seus serviços de pesquisa WHOIS, independentemente de você tê-los desativado com o Route 53. Para obter informações completas sobre seu domínio, recomendamos que você use o WHOIS fornecido pelo registrador.

Observe o seguinte:

Enviar e-mail para contatos de domínio quando a proteção de privacidade está habilitada

> Se a proteção de privacidade estiver habilitada para o domínio, as informações de contato do registrante, do técnico e administrativo serão substituídas pelas informações de contato do serviço de privacidade do Amazon Registrar. Por exemplo, se o domínio exemplo.com estiver registrado no Amazon Registrar e se a proteção de privacidade estiver habilitada, o valor de E-mail do registrante na resposta a uma consulta WHOIS será semelhante a owner1234@exemplo.com.identity-protect.org.

Para entrar em contato com um ou mais contatos de domínio quando a proteção de privacidade estiver habilitada, envie um e-mail para os endereços de e-mail correspondentes. Encaminhamos automaticamente seu e-mail para o contato aplicável.

Denunciar abuso

Para denunciar qualquer atividade ilegal ou violação da Política de uso aceitável, incluindo conteúdo inapropriado, phishing, malware ou spam, envie um e-mail para abuse@amazon.com.

Para visualizar informações sobre domínios registrados no Route 53

1. Em um navegador da Web, acesse um dos seguintes sites:
   - Amazon Registrar WHOIS: https://registrar.amazon.com/whois
   - Amazon Registrar RDAP: https://registrar.amazon.com/rdap
   - Gandi WHOIS: https://whois.gandi.net
2. Insira o nome do domínio sobre o qual você deseja visualizar informações e escolha Search (Pesquisar).

Excluir um registro de nome de domínio

A maioria dos domínios de nível superior (TLDs) permite a exclusão do registro quando ele não é mais necessário. Se for possível excluir o registro, execute o procedimento descrito neste tópico.

Observe o seguinte:

A taxa de registro não é reembolsável

Se você excluir um registro de nome de domínio antes da data programada da validade dele, a taxa de registro não será reembolsada pela AWS .

Os TLDs que permitem que você exclua um registro de domínio

Para determinar se você pode excluir o registro do seu domínio, consulte Domínios que você pode registrar com o Amazon Route 53. Se a seção do TLD não incluir uma subseção "Exclusão de registro de domínio", você poderá excluir o domínio. Antes de excluir o domínio, certifique-se de ter desabilitado o bloqueio de domínio. Para obter mais informações sobre como desativar o bloqueio de domínio, consulte DisableDomainTransferLock.

E se você não puder excluir um registro de domínio?

Se o registro do domínio não permitir que você exclua um registro de nome de domínio, você deverá esperar que o domínio expire. Para garantir que o domínio não seja renovado automaticamente, desabilite a renovação automática do domínio. Quando a data Expires on (Expira em) for atingida, o Route 53 excluirá automaticamente o registro do domínio. Para obter informações sobre como alterar a configuração de renovação automática, consulte Habilitar ou desabilitar a renovação automática de um domínio.

O atraso antes de um domínio é excluído e fica disponível para registro novamente

Quase todos os registros impedem que alguém registre imediatamente um domínio que tenha acabado de expirar. O atraso típico é de um a três meses, dependendo do TLD. Para obter mais informações, consulte a seção "Prazos para renovação e restauração de domínios" para seu TLD em Domínios que você pode registrar com o Amazon Route 53.

> **Important**
>
> Não exclua um domínio e espere registrá-lo novamente se quiser apenas transferir o domínio entre AWS contas ou transferir o domínio para outro registrador. Consulte a documentação aplicável.
>
> - Transferir um domínio para uma conta diferente AWS
> - Como transferir um domínio do Amazon Route 53 para outro registrador

Para excluir um registro de nome de domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do seu domínio.

   Se você desejar excluir um domínio .co.uk, .me.uk, .org.uk ou .uk, consulte Para excluir registros de nomes de domínio.co.uk, .me.uk, .org.uk e .uk.
4. Se o registro do seu TLD permitir a exclusão de um registro de nome de domínio, escolha Excluir domínio.

Alguns domínios podem exigir que enviemos um e-mail ao registrante do domínio para verificar se ele deseja excluí-lo. Se você receber um e-mail, ele será enviado de um dos seguintes endereços de e-mail:

- noreply@registrar.amazon.com: para TLDs registrados pelo Amazon Registrar.
- noreply@domainnameverification.net: para TLDs registrados por nosso associado registrador, Gandi.

Para determinar quem é o registrador do seu TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

5. Se receber o e-mail de verificação, escolha o link no e-mail e aprove ou rejeite a solicitação para excluir o domínio.

> **Important**
>
> O contato do registrante deve seguir imediatamente as instruções no e-mail, ou devemos cancelar a solicitação de exclusão logo após um dia, conforme exigido pela ICANN.

Você receberá outro e-mail quando seu domínio for excluído. Para determinar o status atual da sua solicitação, consulte Visualizar o status do registro de um domínio.

6. Exclua os registros na zona hospedada para o domínio excluído e, em seguida, exclua a zona hospedada. Depois de excluir a zona hospedada, o Route 53 interromperá o faturamento da taxa mensal de uma zona hospedada. Para obter mais informações, consulte a seguinte documentação do :

   - Excluir registros
   - Excluir uma zona hospedada pública
   - Preço do Route 53

7. Se você tiver problemas ao excluir um registro de nome de domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Para excluir registros de nomes de domínio.co.uk, .me.uk, .org.uk e .uk

Se você quiser excluir um domínio .co.uk, .me.uk, .org.uk ou .uk, crie uma conta na Nominet, o registro dos domínios.uk. Para obter mais informações, consulte "Cancelling your domain name" no site da Nominet, https://www.nominet.uk/domain-support/.

> **Important**
>
> Se você excluir (cancelar) um nome de domínio .uk, ele será excluído até o final do dia e estará disponível para qualquer pessoa registrar. Se você quiser apenas transferir o domínio, não o exclua.

Aqui está uma visão geral do processo:

1. No site da Nominet, siga as instruções para fazer login pela primeira vez. Consulte https://secure.nominet.org.uk/auth/login.html. A Nominet envia a você um e-mail com instruções para criar uma senha.
2. Siga as instruções no e-mail que você receber da Nominet.
3. Faça login no site da Nominet e siga as instruções para cancelar (excluir) um nome de domínio.

Entrar em contato com o AWS Support sobre problemas de registro de domínio

AWS fornece um plano de suporte básico, gratuito, para todos os AWS clientes. O plano inclui assistência para os seguintes problemas relacionados ao registro de domínio:

- Transferência do domínio para ou do Amazon Route 53
- Transferência de domínios entre contas AWS
- Aumento de cotas em entidades do Route 53, como o número de domínios que podem ser registrados (Consulte Cotas).
- Alteração do proprietário de um domínio
- Alteração de informações de contato do proprietário de um domínio
- Reenvio de e-mails de confirmação e autorização
- Renovação de domínios

- Restauração de domínios expirados
- Como obter informações sobre faturamento do Route 53
- Fornecimento de prova de identidade para domínios .uk
- Excluindo domínios ou desativando a renovação automática depois de fechar sua conta AWS

Para entrar em contato com o AWS Support sobre esses e outros problemas relacionados ao registro de domínio, execute o procedimento aplicável.

Tópicos

Entrar em contato com o AWS Support quando você pode entrar em sua AWS conta

Para entrar em contato com o AWS Support quando você conseguir entrar em sua AWS conta, execute o procedimento a seguir:

1. Usando a AWS conta na qual o domínio está registrado atualmente, entre no AWS Support Center.

   > **Important**
   >
   > É necessário fazer login usando a conta raiz na qual o domínio está atualmente registrado. Esse requisito impede que usuários não autorizados sequestrem sua conta.

2. Especifique os seguintes valores:

   Referente

   Aceite o valor padrão de Atendimento ao cliente.

   Serviço

   Aceite o valor padrão de Domínios.

   Categoria

   Aceite o valor padrão de Emissão de registro.

Gravidade

Escolha a gravidade aplicável.

Sujeito

Insira um breve resumo do problema.

Descrição

Descreva o problema em mais detalhes e anexe todos os documentos ou capturas de tela relevantes.

Método de contato

Escolha o método de contato, Web. Entraremos em contato com você usando o endereço de e-mail associado à sua AWS conta.

3. Selecione Enviar.

Entrar em contato com o AWS Support quando você não consegue entrar na sua AWS conta

Para entrar em contato com o AWS Support quando você não consegue entrar em sua AWS conta, execute o procedimento a seguir:

1. Acesse a página Sou um AWS cliente e estou procurando a página de suporte para cobrança ou conta.
2. Preencha o formulário.
3. Selecione Enviar.

Fazer download de um relatório de faturamento de domínios

Se sua AWS fatura for cobrada em um cartão de crédito, você receberá uma fatura separada para cada transação de domínio. Essas faturas não incluem o nome de domínio. Se você gerencia vários domínios e quer visualizar as cobranças por domínio para um período especificado, faça download de um relatório de faturamento de domínios. Esse relatório inclui todas as cobranças que se aplicam a registros de domínios, incluindo:

- Registro de um domínio

- Renovação do registro de um domínio
- Como transferir um domínio para o Amazon Route 53
- Alteração do proprietário de um domínio (para alguns TLDs, essa operação é gratuita)

> **Note**
>
> Se você usar pagamentos faturados, todas as transações de registro de domínio do Route 53 aparecerão em sua fatura mensal AWS . A fatura inclui o nome de domínio e a operação a que cada cobrança se aplica.

Às vezes, seu relatório de cobrança pode mostrar períodos de cobrança futuros. Isso acontece porque o processo de renovação automática do domínio começa um mês antes da expiração do domínio. Portanto, por exemplo, em seu relatório de agosto, você poderá ver um período de cobrança que começa em setembro seguinte e vai até setembro do ano seguinte.

Ao gerar o relatório usando o console, é possível escolher as seguintes opções:

- Últimos 12 meses: o relatório inclui cobranças de um ano antes de você executá-lo até a data atual. Por exemplo, se você gerar o relatório em 3 de junho, ele incluirá as cobranças de 3 de junho do ano anterior até a data atual.
- Meses individuais no último ano: o relatório inclui cobranças para o mês especificado.

Se gerar o relatório de forma programática, você poderá obter as cobranças para qualquer intervalo de datas, a partir de 31 de julho de 2014. Esta é a data em que o Route 53 começou a oferecer suporte ao registro de domínio. Por exemplo, consulte exibir-faturamento na Referência de comando da AWS CLI .

O relatório de faturamento, no formato CSV, inclui os seguintes valores:

- O ID da AWS fatura em que a cobrança aparece.
- A operação (REGISTER_DOMAIN, RENEW_DOMAIN, TRANSFER_IN_DOMAIN ou CHANGE_DOMAIN_OWNER).
- O nome do domínio.
- A cobrança pela operação em dólares americanos.

- A data e a hora no formato ISO 8601, por exemplo, 2016-03-03T19:20:25.177Z. Para obter mais informações sobre o formato ISO 8601, consulte o artigo da Wikipédia ISO 8601.

Para fazer download de um relatório de faturamento de domínios

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha Relatório de faturamento de domínios.
4. Escolha o período do relatório e, em seguida, escolha Fazer download do relatório de domínios.
5. Siga as instruções para abrir ou salvar o relatório.
6. Se você tiver problemas ao baixar um relatório de cobrança de domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Domínios que você pode registrar com o Amazon Route 53

> **Important**
>
> O serviço DNS do Route 53 pode ser usado com qualquer domínio de primeiro nível que você escolher e com qualquer registrador de domínio. As informações nesta página se referem somente aos domínios que você pode registrar no Route 53. Para obter mais informações sobre o Route 53 como um serviço DNS, consulte. Como o tráfego da Internet é roteado para seu site ou o aplicativo web

As listas a seguir de domínios de nível superior genéricos e geográficos mostram os domínios de nível superior (TLDs) que você pode utilizar para registrar domínios no Amazon Route 53.

Como registrar domínios com o Route 53

Os registros de TLD atribuíram preços especiais ou premium a alguns nomes de domínio. Não é possível usar o Route 53 para registrar um domínio que tenha um preço especial ou premium. Os TDLs que você poderá registrar com o Route 53 estão incluído nas listas a seguir. Se o TLD não estiver incluído, você não poderá registrar o domínio com o Route 53.

Como transferir domínios para o Route 53

Você poderá transferir um domínio para o Route 53 se o TLD estiver incluído nas listas a seguir. Se o TLD não estiver incluído, não será possível transferir o domínio para o Route 53.

Para a maioria dos TLDs, você precisa obter um código de autorização do registrador atual para transferir um domínio. Para determinar se você precisa de um código de autorização, consulte a seção “Código de autorização necessário para transferir para o Route 53” do TLD.

Definição de preço para o registro e a transferência de domínios

Para obter informações sobre o custo para registrar ou transferir domínios para o Route 53, consulte Preço do Amazon Route 53 para registro de domínio.

Usar o Route 53 como seu serviço DNS

Você pode usar o Route 53 como serviço DNS de qualquer domínio, mesmo que o TLD do domínio não esteja incluído nas listas a seguir. Para obter mais informações sobre o Route 53 como um serviço DNS, consulte Como o tráfego da Internet é roteado para seu site ou o aplicativo web. Para obter informações sobre como transferir o serviço DNS do seu domínio para o Route 53, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Nomes de domínio internacionalizados

Nem todos os TLDs oferecem suporte a nomes de domínio internacionalizados (IDNs), ou seja, nomes de domínio que incluem caracteres diferentes dos caracteres ASCII a-z, 0-9 e - (hífen). A listagem de cada TLD indica se esse TLD oferece suporte a IDNs. Para obter mais informações sobre nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Registrar domínios geográficos com TLDs

As regras para o registro de TLDs geográficos variam de acordo com o país. Alguns países são irrestritos, ou seja, qualquer pessoa no mundo pode registrar. Já outros têm algumas restrições, como residência. A listagem de cada TLD geográfico indica quaisquer restrições.

Índice para domínios de nível superior compatíveis

Tópicos

Domínios genéricos de nível superior

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, .cerveja,.bet, .oferta, .bike, .bingo, .biografia, .biz, .black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .natal, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contato, .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, .ventilador, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .diversão, .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, .lei, .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, .compras, .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, .votar, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .trabalho, .works, .world, .wtf, .xyz, .zone

Domínios geográficos de nível superior

África

.ac (Ilha de Ascensão), .co.za (África do Sul), .sh (Santa Helena)

Américas

.ca (Canadá), .cl (Chile), .co (Colômbia), .com.ar (Argentina), .com.br (Brasil), com.mx (México), .mx (México), .us (Estados Unidos), .vc (São Vicente e Granadinas), .vg (Ilhas Virgens Britânicas)

Ásia/Oceania

.au (Austrália), .cc [Ilhas Cocos (Ilhas Keeling)], .co.nz (Nova Zelândia), .com.au (Austrália), .com.sg (República de Singapura), .fm (Estados Federados da Micronésia), .in (Índia), JP (Japão), .io (Território Britânico do Oceano Índico), .net.au (Austrália), .net.nz (Nova Zelândia), .org.nz (Nova Zelândia), .pw (Palau), .qa (Catar), .ru (Federação Russa), .sg (República de Singapura)

Europa

.be (Bélgica), .berlin (cidade de Berlim na Alemanha), .ch (Suíça), .co.uk (Reino Unido), .cz (República Tcheca), .de (Alemanha), .es (Espanha) , .eu (União Europeia), .fi (Finlândia), .fr (França), .gg (Guernsey), .im (Ilha de Man), .it (Itália), .me (Montenegro), .me.uk (Reino Unido), .nl (Holanda), .org.uk (Reino Unido), .ruhr (região de Ruhr, parte ocidental da Alemanha), .se (Suécia), .uk (Reino Unido), .wien (cidade de Viena, na Áustria)

Domínios genéricos de nível superior

Os domínios genéricos de nível superior (gTLDs) são extensões globais usadas e reconhecidas em todo o mundo, por exemplo, .com, .net e .org. Também estão incluídos os domínios especializados, como .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, .cerveja, .bet, .oferta, .bike, .bingo, .biografia, .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, .natal, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contato, .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, .ventilador, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .diversão, .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, .lei, .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, .compras, .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, .votar, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .trabalho, .works, .world, .wtf, .xyz, .zone

.ac

Consulte .ac (Ilha de Ascensão).

Return to index

.academy

Usada por instituições educacionais, como escolas e universidades. Ela também é usada por recrutadores, consultores, anunciantes, alunos, professores e administradores afiliados a instituições educacionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.accountants

Usada por empresas, grupos e indivíduos afiliados à contabilidade.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.actor

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.adult

Usada para sites que hospedam conteúdo somente para adultos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.agency

Usada por qualquer empresa ou grupo identificado como agência.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.airforce

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.apartments

Usada por corretores de imóveis, proprietários e inquilinos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.associates

Usada por empresas e firmas que incluem o termo "associados" em seus títulos. Ela também é usada por grupos ou agências que desejam indicar a natureza profissional de suas organizações.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.auction

Usada para eventos relacionados a leilões, além de compras e vendas baseadas em leilões.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, espanhol e latim.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.audio

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .audio ou transferir domínios .audio para o Route 53. Continuaremos a oferecer suporte a domínios .audio que já estão registrados no Route 53.

Usada pelo setor audiovisual e por indivíduos interessados em transmissão, equipamentos de som, produção e streaming de áudio.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .audio para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.band

Usada para compartilhar informações sobre bandas e seus eventos. Ela também é usada pelos músicos para interagir com sua base de fãs e vender produtos relacionados à banda.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, espanhol e latim.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.bargains

Usada para obter informações sobre vendas e promoções.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cerveja

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.bet

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.oferta

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.bike

Usada por empresas ou grupos que atendem a ciclistas, como lojas de bicicletas, concessionárias de motocicletas e oficinas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.bingo

Usada para sites de jogos online ou para compartilhar informações sobre jogos de bingo.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.biografia

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.biz

Usada para fins comerciais ou de negócios.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês simplificado, chinês tradicional, dinamarquês, finlandês, alemão, húngaro, japonês, coreano, letão, lituano, norueguês, polonês, português, espanhol e sueco.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.black

Usada por indivíduos que gostam da cor preta ou que desejam associá-la aos seus negócios ou à sua marca.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.blue

Usada por indivíduos que gostam da cor azul ou que desejam associá-la aos seus negócios ou à sua marca.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.boutique

Usada para obter informações sobre butiques e pequenas lojas especializadas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.builders

Usada por empresas e indivíduos afiliados ao setor de construção.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.business

Usada por qualquer tipo de empresa. Ela pode ser usada como uma alternativa à extensão .biz.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.buzz

Usada para obter informações sobre as últimas notícias e eventos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cab

Usada por empresas e indivíduos afiliados ao setor de táxi.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cafe

Usada por empresas de café e por indivíduos que têm interesse na cultura do café.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.camera

Usada por entusiastas de fotografia e por qualquer pessoa que deseja compartilhar fotos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.camp

Usada por parques e departamentos de recreação, acampamentos de verão, workshops de escritores, acampamentos fitness e entusiastas de acampamento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.capital

Usada como uma categoria geral que descreve qualquer tipo de capital, como capital financeiro ou o capital de uma cidade.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cards

Usada por empresas especializadas em cartões, como ecards, cartões de boas-vindas impressos, cartões de visita e cartas de baralho. Ela também é ideal para jogadores que desejam discutir as regras e estratégias dos jogos de cartas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.care

Usada por empresas ou agências de cuidadores. Ela também é usada por organizações de caridade.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.careers

Usada para obter informações sobre recrutamento de profissionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cash

Usada por qualquer organização, grupo ou indivíduo envolvido em atividades relacionadas a dinheiro.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.casino

Usada pelo setor de jogos de azar ou por jogadores que desejam compartilhar informações sobre jogos de azar e de cassino.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.catering

Usada por empresas de buffet ou por indivíduos que compartilham informações sobre eventos relacionados a alimentos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cc

Consulte .cc [Ilhas Cocos (Ilhas Keeling)].

Return to index

.center

Usada como uma extensão genérica para tudo, de organizações de pesquisa a centros comunitários.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade

- O domínio é excluído do registro: 75 dias após a validade

.ceo

Usada para obter informações sobre CEOs e seus equivalentes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para alemão.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.chat

Usada por qualquer tipo de site de chat online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cheap

Usada por sites de comércio eletrônico para promover e vender produtos baratos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.natal

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 43 dias após a expiração
- O domínio é excluído do Route 53: 44 dias após a validade
- A restauração com o registro é possível: entre 44 dias e 86 dias após a expiração
- O domínio é excluído do registro: 86 dias após a expiração

.church

Usada por igrejas de qualquer tamanho ou denominação para se conectar com suas congregações e publicar informações sobre atividades e eventos relacionados a igrejas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.city

Usada para fornecer informações sobre aspectos específicos de cidades, como pontos de interesse, principais atrações locais ou atividades da vizinhança.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.claims

Usada por empresas que gerenciam solicitações de seguro ou fornecem serviços jurídicos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cleaning

Usada por empresas ou indivíduos que fornecem serviços de limpeza.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.click

Usada por empresas que desejam associar a ação de clicar aos seus sites, por exemplo, a ação de clicar em produtos em um site para comprá-los.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Compatível.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.clinic

Usada pelo setor de assistência médica e por profissionais de medicina.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.clothing

Usada pelo setor de moda, incluindo varejistas, lojas de departamentos, designers, alfaiates e outlets.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cloud

Usada como uma extensão geral, mas é ideal para empresas que fornecem serviços e tecnologias de computação em nuvem.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.club

Usada por qualquer tipo de clube ou organização.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para espanhol e japonês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.coach

Usada por qualquer pessoa interessada em treinamento, como profissionais do esporte, coaches pessoais ou instrutores corporativos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.codes

Usada como uma extensão genérica para todos os tipos de código, como códigos de conduta, de construção ou de programação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.coffee

Usada pelo setor de café.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.college

Usada por instituições educacionais, como escolas e universidades. Ela também é usada por recrutadores, consultores, anunciantes, alunos, professores e administradores afiliados a instituições educacionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, chinês simplificado e tradicional, cirílico, grego, hebraico, japonês e tailandês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.com

Usada para sites comerciais. Ela é a extensão mais popular da Internet.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.community

Usada por qualquer tipo de comunidade, clube, organização ou grupo de interesses especiais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.company

Usada como uma extensão genérica para empresas de todos os tipos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.computer

Usada como uma extensão genérica para obter informações sobre computadores.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.condos

Usada por empresas e indivíduos associados a condomínios.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.construction

Usada pelo setor de construção, como construtoras e empreiteiras.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.consulting

Usada por consultores e outros profissionais afiliados ao setor de consultoria.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, chinês, francês, cirílico, devanagari, alemão, grego, hebraico, japonês, coreano, latim, espanhol, tâmil e tailandês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.contato

Usada por igrejas de qualquer tamanho ou denominação para se conectar com suas congregações e publicar informações sobre atividades e eventos relacionados a igrejas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.contractors

Usada por empreiteiras, como as do setor de construção.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cool

Usada por organizações e grupos que desejam associar sua marca às últimas tendências.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.coupons

Usada por varejistas e fabricantes que fornecem cupons e códigos de cupom online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.credit

Usada pelo setor de crédito.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.creditcard

Usada por empresas ou bancos que emitem cartões de crédito.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.cruises

Usada pelo setor de viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.dance

Usada por bailarinos, instrutores e escolas de dança.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.dating

Usada para sites de encontros.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.deals

Usada para fornecer informações sobre vendas e barganhas online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.degree

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.delivery

Usada por empresas que fornecem qualquer tipo de produto ou serviço.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.democrat

Usada para obter informações sobre o Partido Democrata. Ela também é usada por candidatos a mandatos eletivos, autoridades eleitas, entusiastas de política, consultores e conselheiros.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.dental

Usada por profissionais de odontologia e fornecedores de suprimentos odontológicos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.design

Usada por igrejas de qualquer tamanho ou denominação para se conectar com suas congregações e publicar informações sobre atividades e eventos relacionados a igrejas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.diamonds

Usada por entusiastas de diamantes e indivíduos envolvidos no setor de diamantes, incluindo vendedores, revendedores e comerciantes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.diet

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .diet ou transferir domínios .diet para o Route 53. Continuaremos a oferecer suporte a domínios .diet que já estão registrados no Route 53.

Usada por profissionais de saúde e fitness.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .diet para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.digital

Usada para tudo que é digital, mas ideal para empresas de tecnologia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.direct

Usada como uma extensão geral, mas ideal para quem vende produtos diretamente para os clientes por meio de um site de comércio eletrônico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.directory

Usada pelo setor de mídia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.discount

Usada para sites de descontos e empresas que reduzem preços.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.dog

Usada por amantes de cachorros e fornecedores de serviços e produtos para cães.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.domains

Usada para obter informações sobre nomes de domínio.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.education

Usada para obter informações sobre educação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.email

Usada para obter informações sobre a promoção de e-mails.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.energy

Usada como uma extensão geral, mas ideal para quem atua nos campos de energia ou economia de energia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.engineering

Usada por empresas e profissionais de engenharia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.enterprises

Usada para obter informações sobre empresas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.equipment

Usada para obter informações sobre equipamentos, varejistas ou fabricantes de equipamentos e locadoras.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.estate

Usada para obter informações sobre habitação e o setor de habitação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.events

Usada para obter informações sobre eventos de todos os tipos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.exchange

Usada para qualquer tipo de troca: a troca de mercadorias ou até mesmo a simples troca de informações.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.expert

Usada por indivíduos com conhecimentos especializados em diversos campos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.exposed

Usada como uma extensão genérica para diversos assuntos, incluindo fotografia, tabloides e jornalismo investigativo.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.express

Usada como uma extensão geral, mas ideal para quem deseja enfatizar a entrega rápida de bens ou serviços.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fail

Usada por qualquer pessoa que cometeu erros, mas ideal para a publicação de tolices e gafes bem-humoradas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ventilador

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.farm

Usada pelo setor agrícola, como agricultores e engenheiros agrícolas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.finance

Usada pelo setor financeiro.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.financial

Usada pelo setor financeiro.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fish

Usada como uma extensão geral, mas ideal para sites relacionados a peixes e pescaria.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fitness

Usada para promover assuntos sobre fitness e serviços de fitness.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.flights

Usada por agentes de viagens, companhias aéreas e qualquer pessoa afiliada ao setor de viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.florist

Usada por floristas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.flowers

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .flowers ou transferir domínios .flowers para o Route 53. Continuaremos a oferecer suporte a domínios .flowers que já estão registrados no Route 53.

Usada para qualquer assunto relacionado a flores, como a venda de flores online ou informações sobre o cultivo de flores.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .flowers para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fm

Consulte .fm (Estados Federados da Micronésia).

Return to index

.football

Usada por qualquer pessoa envolvida com futebol americano.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.forsale

Usada para a venda de bens e serviços.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.foundation

Usada por organizações sem fins lucrativos, instituições de caridade e outros tipos de fundações.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.diversão

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fund

Usada como uma extensão geral para tudo que estiver relacionado a financiamentos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.furniture

Usada por fabricantes e vendedores de móveis e por qualquer pessoa afiliada ao setor de mobília.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.futbol

Usada para obter informações sobre futebol.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.fyi

Usada como uma extensão geral, mas ideal para compartilhar informações de todos os tipos. "PSI" é o acrônimo de "para sua informação".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gallery

Usada por proprietários de galerias de arte.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.games

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gift

Usada por empresas ou organizações que vendem presentes ou fornecem serviços relacionados a presentes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gifts

Usada por empresas ou organizações que vendem presentes ou fornecem serviços relacionados a presentes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gives

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.glass

Usada pelo setor de vidro, como cortadores de vidro e instaladores de janelas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.global

Usada por empresas ou grupos com um mercado ou uma visão internacional.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, bielorrusso, bósnio, búlgaro, chinês (simplificado), chinês (tradicional), dinamarquês, alemão, hindi, húngaro, islandês, coreano, letão, lituano, macedônio, montenegrino, polonês, russo, sérvio, espanhol, sueco e ucraniano.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gmbh

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gold

Usada como uma extensão geral, mas ideal para empresas que compram ou vendem ouro ou produtos relacionados a ouro.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.golf

Usada para sites dedicados ao golfe.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.graphics

Usada pelo setor gráfico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gratis

Usada para sites que oferecem produtos gratuitos, como itens promocionais, downloads ou cupons. "Grátis" é uma palavra espanhola que significa "gratuito".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.green

Usada para sites dedicados à conservação, à ecologia, ao meio ambiente e ao estilo de vida ecológico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.gripe

Usada para compartilhar reclamações e críticas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.group

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.guide

Usada como uma extensão geral, mas ideal para sites focados em destinos de viagens, serviços e produtos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.guitars

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .guitars ou transferir domínios .guitars para o Route 53. Continuaremos a oferecer suporte a domínios .guitars que já estão registrados no Route 53.

Usada por entusiastas de guitarras.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .guitars para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.guru

Usada por quem deseja compartilhar seus conhecimentos sobre diversos assuntos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.haus

Usada pelos setores de imóveis e construção. "Haus" é uma palavra alemã que significa "casa".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.healthcare

Usado pelo setor de assistência médica.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.help

Usada como uma extensão geral, mas ideal para sites que fornecem ajuda e informações online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.hiv

Usada para sites dedicados à luta contra o HIV.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.hockey

Usada para sites dedicados ao hóquei.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.holdings

Usada por consultores financeiros, corretores e pessoas que trabalham com investimentos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.holiday

Usada pelo setor de viagens e por empresas e indivíduos envolvidos no planejamento de eventos e ocasiões especiais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.host

Usada por empresas que fornecem plataformas e serviços de hospedagem na web.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, chinês simplificado, chinês tradicional, grego, hebraico, coreano e tailandês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.hosting

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .hosting ou transferir domínios .hosting para o Route 53. Continuaremos a oferecer suporte a domínios .hosting que já estão registrados no Route 53.

Usada para sites de hospedagem ou pelo setor de hospedagem.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .hosting para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.house

Usada por corretores de imóveis, compradores e vendedores de casas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade

- O domínio é excluído do registro: 75 dias após a validade

.im

Consulte .im (Ilha de Man).

Return to index

.immo

Usada pelo setor imobiliário.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade

- O domínio é excluído do registro: 75 dias após a validade

.immobilien

Usada para obter informações sobre imóveis.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.industries

Usada por qualquer empresa ou comércio que deseja se identificar como um setor.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.info

Usada para a disseminação de informações.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ink

Usada por entusiastas de tatuagens ou por qualquer setor relacionado a tintas, como os setores de impressão e publicação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe e latim.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.institute

Usada por qualquer organização ou grupo, especialmente organizações educacionais e de pesquisas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.insure

Usada por companhias e corretores de seguros.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.international

Usada por empresas que possuem cadeias internacionais, indivíduos que viajam para o exterior ou organizações de caridade com influência internacional.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.investments

Usada como uma extensão geral, mas ideal para promover oportunidades de investimento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.io

Consulte .io (Território Britânico do Oceano Índico).

Return to index

.irish

Usada para promover a cultura e as organizações irlandesas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, chinês simplificado, chinês tradicional, francês, alemão, grego, hebraico, japonês, coreano, espanhol, tâmil e tailandês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.jewelry

Usada por vendedores e compradores de joias.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.juegos

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .juegos ou transferir domínios .juegos para o Route 53. Continuaremos a oferecer suporte a domínios .juegos que já estão registrados no Route 53.

Usada para sites de jogos de todos os tipos. "Juegos" é uma palavra espanhola que significa "jogos".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .juegos para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.kaufen

Usada para obter informações sobre comércio eletrônico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.kim

Usada por pessoas cujo nome ou sobrenome é Kim.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.kitchen

Usada por varejistas de utensílios para cozinha, cozinheiros, blogueiros especializados em alimentação e qualquer pessoa do setor de alimentação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.kiwi

Usada por empresas e indivíduos que desejam apoiar a cultura de kiwi da Nova Zelândia. Ela também é usada como uma plataforma de ajuda humanitária para a reconstrução da Christchurch, danificada por terremotos em 2010 e 2011.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para maori.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.land

Usada por agricultores, corretores de imóveis, desenvolvedores comerciais e por qualquer pessoa interessada em propriedades.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.lei

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.lease

Usada por corretores de imóveis, proprietários e inquilinos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.legal

Usada por juristas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.lgbt

Usada pela comunidade de lésbicas, gays, bissexuais e transexuais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.life

Usada como uma extensão geral. Ela é adequada para uma grande variedade de empresas, grupos e indivíduos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.lighting

Usada por fotógrafos, designers, arquitetos, engenheiros e outras pessoas com interesse em iluminação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.limited

Usada como uma extensão geral. Ela é adequada para uma grande variedade de empresas, grupos e indivíduos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.limo

Usada por motoristas, empresas de limusines e locadoras de carros.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.link

Usada para obter informações sobre a criação de links para atalhos online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Uniregistry é o registro para os domínios .LINK. Devido à política do Uniregistry, o nível de registro WHOISmostra "REDACTED FOR PRIVACY" (OCULTADO PARA PRIVACIDADE). A remoção de nosso recurso de proteção de privacidade afetará apenas as informações exibidas no nível do registrador Amazon Registrar WHOIS.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.live

Usada como uma extensão geral. Ela é adequada para uma grande variedade de empresas, grupos e indivíduos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.llc

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.loan

Usada por credores, mutuários e profissionais de crédito.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para dinamarquês, alemão, norueguês e sueco.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.loans

Usada por credores, mutuários e profissionais de crédito.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.lol

Usada para sites de humor e comédia. "LOL" é um acrônimo para "laugh out loud" (risos em voz alta).

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico, francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ltd

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.maison

Usada pelo setor imobiliário.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.management

Usada para obter informações sobre o mundo dos negócios e o gerenciamento de empresas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.marketing

Usada pelo setor de marketing para diversas finalidades.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.mba

Usada para sites que fornecem informações sobre o título de mestre em administração de empresas (MBA).

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.media

Usada pelos setores de mídia e entretenimento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.memorial

Usada por organizações comemorativas dedicadas a homenagear eventos e pessoas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.mobi

Usada por empresas e indivíduos que desejam disponibilizar o acesso aos seus sites em celulares.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.moda

Usada para obter informações sobre moda.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.money

Usada para sites focados em dinheiro e atividades relacionadas a dinheiro.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.mortgage

Usada pelo setor de hipoteca.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.movie

Usada para sites que fornecem informações sobre filmes e produção de filmes. Adequada para profissionais e fãs.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.name

Usada por qualquer pessoa que deseja criar uma presença personalizada na web.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Verisign, o registro de TLDs .name, permite registrar domínios de segundo nível (name.name) (nome.nome) e domínios de terceiro nível (firstname.lastname.name) (nome.sobrenome.nome). O Route 53 oferece suporte apenas a domínios de segundo nível, tanto para registrar domínios quanto para transferir os domínios existentes para o Route 53.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.net

Usada para todos os tipos de sites. A extensão .net é uma abreviação de rede.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

network

Usada por indivíduos do setor de rede ou que desejam criar conexões por meio de redes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.news

Usada para distribuir qualquer notícia, como eventos atuais ou informações relacionadas ao jornalismo e à comunicação.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ninja

Usada por indivíduos e empresas que desejam se associar às habilidades de um ninja.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.onl

A extensão .onl é uma abreviação para "online" e também é a forma abreviada em espanhol para "organização sem fins lucrativos".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, bielorrusso, bósnio, búlgaro, chinês (simplificado e tradicional), dinamarquês, alemão, hindi, húngaro, islandês, coreano, lituano, letão, macedônio, polonês, russo, sérvio e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.online

A extensão .onl é uma abreviação para "online" e também é a forma abreviada em espanhol para "organização sem fins lucrativos".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.org

Usada por todos os tipos de organizações.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.partners

Usada por escritórios de advocacia, investidores e diversas empresas. Ela também é usada para sites sociais que criam relacionamentos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.parts

Usada como uma extensão geral, mas ideal para fabricantes, vendedores e compradores de peças.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.photo

Usada por fotógrafos e por qualquer pessoa interessada em fotos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.photography

Usada por fotógrafos e por qualquer pessoa interessada em fotos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.photos

Usada por fotógrafos e por qualquer pessoa interessada em fotos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pics

Usada por fotógrafos e por qualquer pessoa interessada em fotos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pictures

Usada por qualquer pessoa interessada em fotografia, arte e mídia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pink

Usada por indivíduos que gostam da cor rosa ou que desejam associá-la aos seus negócios ou à sua marca.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pizza

Usada por pizzarias e amantes de pizza.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.place

Usada como uma extensão geral, mas ideal para os setores de casa e viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.plumbing

Usada pelo setor de encanamento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.plus

Usada como uma extensão geral, mas ideal para moda maior, softwares complementares ou qualquer produto que ofereça recursos ou dimensões adicionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.poker

Usada por jogadores de pôquer e sites de jogos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.porn

Usada para sites somente para adultos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.press

Usada para sites somente para adultos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pro

Usada por profissionais licenciados e credenciados e por organizações profissionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.productions

Usada por estúdios e produtoras que criam comerciais, anúncios de rádio e vídeos de música.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.properties

Usada para obter informações sobre qualquer tipo de propriedade, incluindo imóveis ou propriedade intelectual. Ela também é usada por indivíduos que possuem casas, edifícios ou terras para vender, arrendar ou alugar.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.property

Usada para obter informações sobre qualquer tipo de propriedade, incluindo imóveis ou propriedade intelectual. Ela também é usada por indivíduos que possuem casas, edifícios ou terras para vender, arrendar ou alugar.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .property para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.pub

Usada pelos setores de publicação, publicidade ou fabricação de cerveja.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.qpon

Usada para cupons e códigos promocionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.recipes

Usada por indivíduos que desejam compartilhar receitas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.red

Usada por indivíduos que gostam da cor vermelha ou que desejam associá-la aos seus negócios ou à sua marca.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.reise

Usada para sites relacionados a viagens. "Reise" é uma palavra alemã que significa "aumentar", "elevar" ou "em uma jornada".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.reisen

Usada para sites relacionados a viagens. “Reisen” é um verbo alemão que significa “viajar”.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.rentals

Usada para todos os tipos de aluguéis.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.repair

Usada por serviços de reparos ou por quem deseja ensinar a outras pessoas como reparar todos os tipos de itens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.report

Usada como uma extensão geral, mas ideal para obter informações sobre relatórios de negócios, publicações da comunidade, resenhas ou boletins de notícias.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.republican

Usada para obter informações sobre o Partido Republicano. Ela também é usada por candidatos a mandatos eletivos, autoridades eleitas, entusiastas de política, consultores e conselheiros.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.restaurant

Usada pelo setor de restaurantes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.reviews

Usada por indivíduos que desejam dar opiniões e ler os comentários de outras pessoas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.rip

Usada para sites dedicados à morte e memoriais. "RIP" é um acrônimo para "rest in peace" (descanse em paz).

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.rocks

Usada como uma extensão geral, mas ideal para qualquer pessoa ligada aos seguintes assuntos: músicos, geólogos, joalheiros, alpinistas e muito mais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.run

Usada como uma extensão geral, mas ideal para os setores de fitness e esportes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.sale

Usada por sites de comércio eletrônico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.sarl

Usada por sociedades anônimas normalmente localizadas na França. "SARL" é um acrônimo para Société à Responsabilité Limité.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.school

Usada para obter informações sobre educação, instituições de ensino e atividades relacionadas a escolas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.schule

Usada para obter informações sobre educação, instituições de ensino e atividades relacionadas a escolas na Alemanha. "Schule" é uma palavra alemã que significa "escola".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.services

Usada para sites focados em serviços de qualquer tipo.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.sex

Usada para conteúdos somente para adultos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.sexy

Usada para conteúdo sexual. Ela também é usada para descrever as marcas, produtos, informações e sites mais populares e interessantes.

Return to index

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .sexy ou transferir domínios .sexy para o Route 53. Continuaremos a oferecer suporte a domínios .sexy que já estão registrados no Route 53.

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .sexy para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.shiksha

Usada por instituições de ensino. "Shiksha" é um termo indiano para "escola".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.shoes

Usada por varejistas de sapatos, designers, fabricantes ou blogueiros de moda.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.compras

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.show

Usada como uma extensão geral, mas ideal para o setor de entretenimento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.singles

Usada por serviços de namoro, resorts e outras empresas que atendem a pessoas que desejam estabelecer um relacionamento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.site

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ski

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.soccer

Usada para sites dedicados ao futebol.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.social

Usada para obter informações sobre mídias sociais, fóruns de discussão e conversas online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.solar

Usada para obter informações sobre o sistema solar ou energia solar.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.solutions

Usado por consultores, do-it-yourself serviços e conselheiros de todos os tipos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.software

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.space

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.store

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.stream

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.studio

Usada como uma extensão geral, mas ideal para quem atua nos setores imobiliário, de arte ou entretenimento.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.style

Usada como uma extensão geral, mas ideal para sites dedicados às últimas tendências, especialmente em moda, design, arquitetura e arte.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.sucks

Usada como uma extensão geral, mas ideal para quem deseja compartilhar experiências negativas ou alertar outras pessoas sobre fraudes ou produtos com defeito.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.supplies

Usada por empresas que vendem produtos online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.supply

Usada por empresas que vendem produtos online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.support

Usada por empresas, grupos ou instituições de caridade que oferecem qualquer tipo de suporte, incluindo suporte ao cliente, produto ou sistema, além de suporte emocional, financeiro ou espiritual.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.surgery

Usada para obter informações sobre cirurgias, medicina e assistência médica.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.systems

Usada, principalmente, pelo setor de tecnologia e por indivíduos que oferecem serviços de tecnologia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tattoo

Usada por entusiastas e pelo setor de tatuagem.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para cirílico (principalmente russo), francês, alemão, italiano, português e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tax

Usada para obter informações sobre impostos, preparação de declarações de impostos e legislação tributária.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.taxi

Usada por empresas de serviços de táxi, motoristas e transporte.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.team

Usada por qualquer empresa ou organização que deseja se identificar como uma equipe.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tech

Usada por entusiastas de tecnologia e por indivíduos dedicados à tecnologia em empresas, serviços e fabricantes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.technology

Usada por entusiastas de tecnologia e por indivíduos dedicados à tecnologia em empresas, serviços e fabricantes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tennis

Usada para obter informações relacionadas a jogos de tênis.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.theater

Usada para sites dedicados a cinemas, peças e musicais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tienda

Usada por empresas de varejo que desejam se conectar com consumidores que falam espanhol.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tips

Usada por quem deseja compartilhar seus conhecimentos e orientações sobre, praticamente, qualquer tópico.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tires

Usada por fabricantes, distribuidores ou compradores de pneus.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.today

Usada para obter informações sobre eventos atuais, notícias, previsão do tempo, entretenimento e muito mais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tools

Usada para obter informações sobre qualquer tipo de ferramenta.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tours

Usada como uma extensão geral, mas ideal para agências de viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.town

Usada para promover a localidade, a cultura e a comunidade de uma cidade.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.toys

Usada pelo setor de brinquedos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.trade

Usada como uma extensão geral, mas ideal para sites ou serviços de comércio.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para dinamarquês, alemão, norueguês e sueco.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.training

Usada por instrutores, treinadores e educadores.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.tv

Usada para obter informações sobre televisão e mídia.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Nenhum.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.university

Usada por universidades e outras organizações educacionais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.uno

Usada para obter informações sobre comunidades hispânicas, portuguesas e italianas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.vacations

Usada pelos setores de viagens e turismo.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.vegas

Usada para promover a cidade e o estilo de vida de Las Vegas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.ventures

Usada por empreendedores, startups, investidores, bancos de investimento e financistas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.vg

Consulte .vg (Ilhas Virgens Britânicas).

Return to index

.viajes

Usada por agências de viagens, operadores de turismo, blogs de viagens, empresas de turismo, serviços de locação, blogueiros de viagens e varejistas de viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.video

Usada pelos setores de mídia e vídeo.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão, latim e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.villas

Usada por corretores de imóveis e proprietários que possuem casas de campo para vender, alugar ou arrendar.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.vision

Usada como uma extensão geral, mas ideal para especialistas em visão, como optometristas e oftalmologistas.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.votar

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade

- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.voyage

Usada por agências de viagens, operadores de turismo, blogs de viagens, empresas de turismo, serviços de locação, blogueiros de viagens e varejistas de viagens.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.watch

Usada para obter informações sobre sites de streaming, televisão pela Internet ou vídeos.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.website

Usada para obter informações sobre promoção, melhorias, experiências e desenvolvimento de sites.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, chinês simplificado, chinês tradicional, grego, hebraico, japonês, coreano e tailandês.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.wedding

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Nenhum.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para chinês, francês, alemão e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.wiki

Usada para obter informações sobre documentação online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe e latim.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.wine

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção da privacidade

Compatível.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.trabalho

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.works

Usada por empresas, organizações e indivíduos para obter informações sobre trabalho, cargos e serviços de emprego. Essa extensão pode ser usada como uma alternativa às extensões .com, .net ou .org.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.world

Usada por qualquer pessoa que deseja fornecer informações sobre assuntos globais.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.wtf

Usada por qualquer pessoa que deseja se identificar com o acrônimo popular (porém vulgar) "WTF".

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.xyz

Usada como uma extensão geral para qualquer finalidade.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

O registro dos domínios .zyz, Generation XYZ, considera alguns nomes de domínio como nomes de domínio premium. Não é possível registrar domínios .xyz premium com o Route 53 ou transferi-los para ele. Para obter mais informações, consulte o site Generation XYZ.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.zone

Usada para obter informações sobre qualquer tipo de zona, incluindo fusos horários, zonas climáticas e de esportes.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para francês e espanhol.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

Domínios geográficos de nível superior

As extensões de domínio a seguir são agrupadas por região e incluem as extensões oficiais específicas dos países, conhecidas como domínios de nível superior de código do país (ccTLDs). Entre os exemplos estão: .be (Bélgica), .in (Índia) e. mx (México). As regras para o registro de ccTLDs variam de acordo com o país. Alguns países são irrestritos, ou seja, qualquer pessoa no mundo pode registrar. Já outros têm algumas restrições, como residência. A listagem de cada ccTLD indica quaisquer restrições.

> **Important**
>
> Durante a transferência de qualquer ccTLDs para o Route 53, exceto o.cc e .tv, as atualizações do contato do proprietário são ignoradas e os dados de contato do proprietário do registro são usados. Você pode atualizar o contato do proprietário após a conclusão da transferência. Para ter mais informações, consulte Atualizar informações de contato e propriedade de um domínio.

Return to index

África

.ac (Ilha de Ascensão), .co.za (África do Sul), .sh (Santa Helena)

Américas

.ca (Canadá), .cl (Chile), .co (Colômbia), .com.ar (Argentina), .com.br (Brasil), com.mx (México), .mx (México), .us (Estados Unidos), .vc (São Vicente e Granadinas), .vg (Ilhas Virgens Britânicas)

Ásia/Oceania

.au (Austrália), .cc [Ilhas Cocos (Ilhas Keeling)], .co.nz (Nova Zelândia), .com.au (Austrália), .com.sg (República de Singapura), .fm (Estados Federados da Micronésia), .in (Índia), JP (Japão), .io (Território Britânico do Oceano Índico), .net.au (Austrália), .net.nz (Nova Zelândia), .org.nz (Nova Zelândia), .pw (Palau), .qa (Catar), .ru (Federação Russa), .sg (República de Singapura)

Europa

.be (Bélgica), .berlin (cidade de Berlim na Alemanha), .ch (Suíça), .co.uk (Reino Unido), .cz (República Tcheca), .de (Alemanha), .es (Espanha) , .eu (União Europeia), .fi (Finlândia), .fr (França), .gg (Guernsey), .im (Ilha de Man), .it (Itália), .me (Montenegro), .me.uk (Reino Unido), .nl (Holanda), .org.uk (Reino Unido), .ruhr (região de Ruhr, parte ocidental da Alemanha), .se (Suécia), .uk (Reino Unido), .wien (cidade de Viena, na Áustria)

África

É possível usar os domínios de nível superior (TLDs) a seguir para a África com o objetivo de registrar domínios no Amazon Route 53.

, ,

Return to index

.ac (Ilha de Ascensão)

Return to index

Ela também é usada como um TLD genérico popular para ambientes acadêmicos.

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade

- O domínio é excluído do registro: 80 dias após a validade

.co.za (África do Sul)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Somente os domínios de segundo nível estão disponíveis para a extensão .za. O Route 53 oferece suporte ao domínio de segundo nível. co.za.

Aberto ao público, com algumas restrições:

- O registro é aberto para pessoas jurídicas identificáveis (indivíduos e empresas).
- O nome de domínio deve passar por uma verificação de zona durante o processo de registro.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Para evitar transferências não autorizadas, restrinja o acesso ao endereço de e-mail do registrante e às APIs do Route 53 que poderiam permitir a mudança de propriedade, por exemplo, Contato. UpdateDomain Para obter mais informações, consulte Ações, recursos e chaves de condição do Route 53 Domains na Referência de autorização do serviço e Permissões de exemplo para um proprietário de registro de domínio.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Não

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até um dia antes da data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 1 dia antes da validade
- A restauração com o registro é possível: entre 1 e 9 dias após a expiração
- O domínio é excluído do registro: 9 dias após a expiração

.sh (Santa Helena)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração

- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 80 dias após a validade

Américas

É possível usar os domínios de nível superior (TLDs) a seguir para as Américas com o objetivo de registrar domínios no Amazon Route 53.

, , , , , , , , ,

Return to index

.ca (Canadá)

Return to index

Variantes, com (à) ou sem (a) um acento, de um nome de domínio são automaticamente reservadas para o registrante e se tornam parte de um pacote administrativo. Para ativar um domínio em um pacote, o registrante deve fazer uma solicitação de registro para o domínio. Todos os domínios em um pacote devem ser registrados pelo mesmo registrante e pelo mesmo registrador. O registrante também precisará enviar uma solicitação de transferência para todos os domínios em um pacote para concluir a transferência.

E-mail de confirmação do registro do TLD

Ao registrar um domínio .ca, você receberá um e-mail com um link para o procedimento de aceitação do contrato do registrante. É necessário concluir o procedimento dentro de sete dias. Caso contrário, o domínio não será registrado.

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com algumas restrições:

- O registro é aberto para organizações ou indivíduos relacionados ao Canadá, conforme descrito pelo Canadian Presence Requirements for Registrants.

- Contato do registrante: é necessário fornecer a razão social exata e completa do proprietário do domínio.
- Contatos administrativos e de tecnologia: é necessário especificar Pessoa como o tipo de contato e fornecer informações de contato de indivíduos que vivem no Canadá.
- É necessário selecionar um dos tipos jurídicos a seguir durante o processo de registro:
  - ABO: povos aborígenes (indivíduos ou grupos) indígenas do Canadá
  - ASS: associação canadense não incorporada
  - CCO: corporação canadense, província ou território canadense
  - CCT: cidadão canadense
  - EDU: instituição educacional canadense
  - GOV: governo ou entidade governamental no Canadá
  - HOP: hospital canadense
  - INB: bando indígena reconhecido pelo Indian Act of Canada
  - LAM: biblioteca, arquivo ou museu canadense
  - LGR: representante legal de um cidadão canadense ou residente permanente
  - MAJ: sua Majestade, a rainha/rei
  - OMK: marca oficial registrada no Canadá
  - PLT: partido político canadense
  - PRT: parceria registrada no Canadá
  - RES: residente permanente do Canadá
  - TDM: marca comercial registada no Canadá (por um tipo de proprietário não canadense)
  - TRD: sindicato canadense
  - TRS: confiança estabelecida no Canadá

Proteção da privacidade

- Pessoa — Para todos os contatos, o nome, endereço, número de telefone, número de fax e endereço de e-mail do contato ficam ocultos, pois o CIRA aplica automaticamente sua proteção de privacidade a uma pessoa. A opção de proteção de privacidade será aplicada somente no registrador Whois.
- Empresa, associação ou órgão público — Não há suporte no nível do registro.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: varia. Entrar em contato com o AWS Support.

Exclusão de registro de domínio

O registro de domínios .ca não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.cl (Chile)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .cl ou transferir domínios .cl para o Route 53. Continuaremos a oferecer suporte a domínios .cl que já estão registrados no Route 53.

Return to index

Período de renovação

2 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .cl para o Route 53.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre em contato com o AWS Support.
- A renovação tardia com o Route 53 é possível: entre em contato com o AWS Support.
- O domínio foi excluído do Route 53: entre em contato com o AWS Support.
- A restauração com o registro é possível: entre em contato com o AWS Support.
- O domínio é excluído do registro: entre em contato com o AWS Support.

.co (Colômbia)

Return to index

Período de contrato para registro e renovação

De 1 a 5 anos.

Restrições

O registro de domínios .co, Go.co, considera alguns nomes de domínio como nomes de domínio premium. Não é possível registrar domínios .co premium no Route 53 ou transferi-los para ele. Para obter mais informações, consulte o site Go.co.

Proteção de privacidade (aplicável a: pessoa)

Todas as informações são ocultas.

Se o tipo de contato não for uma pessoa, o nome da empresa e o país serão exibidos pelo WHOIS.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 45 dias após a expiração
- O domínio é excluído do registro: 50 dias após a expiração

.com.ar (Argentina)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .com.ar ou transferir domínios .com.ar para o Route 53. Continuaremos a oferecer suporte a domínios .com.ar que já estão registrados no Route 53.

Return to index

Período de renovação

1 ano.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Para evitar transferências não autorizadas, restrinja o acesso ao endereço de e-mail do registrante e às APIs do Route 53 que poderiam permitir a mudança de propriedade, por exemplo, Contato. UpdateDomain Para obter mais informações, consulte Ações, recursos e chaves de condição do Route 53 Domains na Referência de autorização do serviço e Permissões de exemplo para um proprietário de registro de domínio.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .com.ar para o Route 53.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre em contato com o AWS Support.
- A renovação tardia com o Route 53 é possível: entre em contato com o AWS Support.
- O domínio foi excluído do Route 53: entre em contato com o AWS Support.
- A restauração com o registro é possível: entre em contato com o AWS Support.
- O domínio é excluído do registro: entre em contato com o AWS Support.

.com.br (Brasil)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .com.br ou transferir domínios .com.br para o Route 53. Continuaremos a oferecer suporte a domínios .com.br que já estão registrados no Route 53.

Return to index

Período de renovação

1 ano.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .com.br para o Route 53.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: durante os 30 dias anteriores à data de expiração
- A renovação tardia com o Route 53 é possível: até 119 dias após a validade
- O domínio é excluído do Route 53: 119 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 119 dias após a expiração

com.mx (México)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.mx (México)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 75 dias após a validade

.us (Estados Unidos)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

O registro de domínios .us não permite nomes de domínio que contenham qualquer uma das sete palavras identificadas no “Appendix to Opinion of the Court” da Federal Communications Commission v. Pacifica Foundation No. 77-528.

Aberto ao público, com uma restrição:

- A extensão .us é destinada a atividades ou sites localizados nos Estados Unidos da América.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 65 dias após a expiração

.vc (São Vicente e Granadinas)

Ela também é usada como um TLD genérico, frequentemente por pessoas envolvidas em financiamento de capital de risco, universidades e assim por diante.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 80 dias após a validade

.vg (Ilhas Virgens Britânicas)

Ela também é usada como um TLD genérico, frequentemente por organizações envolvidas em videogames.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- É possível fazer a renovação até 44 dias após da data de expiração
- A renovação tardia com o Route 53 é possível: sim
- O domínio é excluído do Route 53: 45 dias após a validade
- O domínio é excluído do registro: 45 dias após a expiração
- A restauração com o registro é possível: entre 45 e 74 dias após a expiração
- O domínio é disponibilizado publicamente novamente: 80 dias após a expiração

Ásia/Oceania

É possível usar os domínios de nível superior (TLDs) a seguir para a Ásia e a Oceania com o objetivo de registrar domínios no Amazon Route 53.

, , , , , , , , , , , , , , ,

Return to index

.au (Austrália)

Return to index

E-mail de confirmação do registro do TLD

Nosso associado registrador, Gandi, revende domínios.au por meio de. DomainDirectors Quando você transfere um nome de domínio para o Route 53, DomainDirectors envia um e-mail para o contato do registrante do domínio para verificar as informações de contato ou autorizar solicitações de transferência.

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, com algumas restrições:

- Os domínios .au são abertos a pessoas jurídicas, comércio, parcerias ou comerciantes registrados na Austrália, a empresas estrangeiras licenciadas para praticar atividades comerciais na Austrália e a proprietários ou requerentes de uma marca registrada da Austrália. Indivíduos não podem registrar domínios .au. O contato do registrante deve ser uma empresa.
- Seu nome de domínio deve ser idêntico ao seu nome, como registrado junto às autoridades australianas relevantes, ou à sua marca comercial (ou à abreviação ou acrônimo dela).
- O nome de domínio deve indicar sua atividade. Por exemplo, ele deve indicar um produto que você vende ou um serviço que fornece.
- Durante o processo de registro, você deve indicar o seguinte:
  - Seu tipo de registro: ABN (Número de registro comercial australiano), ACN (Número de empresa australiana) ou TM (Marca comercial) se o nome do domínio corresponder à sua marca comercial.
  - O número do ID, que pode ser o número de um cartão do Medicare, o número de um arquivo fiscal (TFN), o número da carteira de habilitação ou um Número de registro comercial australiano (ABN).
  - Seu estado ou província.
- Informações de contato incorretas ou incompatíveis, incluindo nome, ABN ou número de marca comercial (TM) resultarão em falhas de registro, comércio e renovações. Uma alteração de propriedade pode ser necessária para corrigir informações para domínios existentes.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Ao definir a chave, você deve escolher o algoritmo de segurança DNS 2 (DH). Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 60 dias antes da expiração e a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 29 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 30 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .au não permite excluir registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

Como alterar uma propriedade

Altere o proprietário usando o console do Route 53. Consulte Atualizar informações de contato de um domínio. Em seguida, conclua o seguinte processo para concluir a alteração da propriedade:

1. Tanto os inscritos antigos quanto os novos devem clicar no link que receberam em um e-mail de transfers@1api.net para os endereços de e-mail listados. Se isso não for concluído em até 14 dias, terá de recomeçar o processo.

2. Após a confirmação das respostas, a alteração do proprietário no registro será processada em pouco tempo sem confirmação adicional.

.cc [Ilhas Cocos (Ilhas Keeling)]

Return to index

Ela também é usada como um TLD genérico, frequentemente por organizações com "cc" em seus nomes, como empresas de consultoria, de computação em nuvem ou clubes de ciclismo. A extensão é uma alternativa popular para ".com".

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

- Hidden (Ocultos): endereço, número de telefone, número de fax e endereço de e-mail
- Not hidden (Não ocultos): nome de contato e organização

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 65 dias após a expiração

.co.nz (Nova Zelândia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Você pode registrar os seguintes domínios de segundo nível com o Route 53: .co.nz, .net.nz e .org.nz. Não é possível registrar domínios .nz (primeiro nível) com o Route 53 nem transferi-los para o Route 53.

Aberto ao público, com algumas restrições:

- Os indivíduos devem ter, pelo menos, 18 anos.
- As organizações devem ser registradas.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 44 dias após a validade

- A restauração com o registro é possível: de 44 a 134 dias após a expiração
- O domínio é excluído do registro: 134 dias após a expiração

.com.au (Austrália)

Return to index

E-mail de confirmação do registro do TLD

Nosso associado registrador, Gandi, revende domínios.com.au por meio de. DomainDirectors Quando você transfere um nome de domínio para o Route 53, DomainDirectors envia um e-mail para o contato do registrante do domínio para verificar as informações de contato ou autorizar solicitações de transferência.

Período de contrato para registro e renovação

De 1 a 5 anos.

Restrições

Aberto ao público, com algumas restrições:

- Os domínios .com.au e .net.au são abertos para empresas, parcerias ou comerciantes registrados na Austrália, para empresas estrangeiras licenciadas para praticar atividades comerciais na Austrália e para proprietários ou requerentes de uma marca registrada da Austrália. Indivíduos não podem registrar domínios .com.au/.net.au. O contato do registrante deve ser uma empresa.
- Seu nome de domínio deve ser idêntico ao seu nome (como registrado junto às autoridades australianas relevantes) ou à sua marca comercial (ou à abreviação ou acrônimo da sua marca comercial).
- O nome de domínio deve indicar sua atividade. Por exemplo, ele deve indicar um produto que você vende ou um serviço que fornece.
- Durante o processo de registro, você deve fornecer as seguintes informações:
  - Seu tipo de registro: ABN (Número de registro comercial australiano), ACN (Número de empresa australiana) ou TM (Marca comercial) se o nome do domínio corresponder à sua marca comercial.
  - Seu número de ID: que pode ser um número de registro comercial australiano (ABN), um número de empresa australiana (ACN) ou a sua marca comercial (TM) se o nome do domínio corresponder à sua marca comercial.

- Seu estado ou província.
- Informações de contato incorretas ou incompatíveis, incluindo nome, ABN ou número de marca comercial (TM) resultarão em falhas de registro, comércio e renovações. Uma alteração de propriedade pode ser necessária para corrigir informações para domínios existentes.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Ao definir a chave, você deve escolher o algoritmo de segurança DNS 2 (DH). Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 60 dias antes da expiração e a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 29 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 30 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .com.au não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

Como alterar uma propriedade

Altere o proprietário de modo programático ou com o console do Route 53. Consulte Atualizar informações de contato de um domínio. Em seguida, conclua o seguinte processo para concluir a alteração da propriedade:

1. Tanto os inscritos antigos quanto os novos devem clicar no link que receberam em um e-mail de transfers@1api.net para os endereços de e-mail listados. Se isso não for concluído em até 14 dias, terá de recomeçar o processo.

2. Após a confirmação das respostas, a alteração do proprietário no registro será processada em pouco tempo sem confirmação adicional.

.com.sg (República de Singapura)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .com.sg ou transferir domínios .com.sg para o Route 53. Continuaremos a oferecer suporte a domínios .com.sg que já estão registrados no Route 53.

Return to index

Período de renovação

Um ou dois anos.

Exclusão de registro de domínio

O registro de domínios .com.sg não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .com.sg para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 60 dias após a expiração

.fm (Estados Federados da Micronésia)

Ela também é usada como um TLD genérico, frequentemente, por organizações envolvidas em transmissões e mídias online.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 44 dias após a validade
- A restauração com o registro é possível: entre 44 e 79 dias após a expiração
- O domínio é excluído do registro: 84 dias após a expiração

.in (Índia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 65 dias após a expiração

JP (Japão)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, com uma restrição:

- Somente indivíduos ou empresas no Japão podem registrar um nome de domínio .jp.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Para evitar transferências não autorizadas, restrinja o acesso ao endereço de e-mail do registrante e às APIs do Route 53 que poderiam permitir a mudança de propriedade, por exemplo, Contato. UpdateDomain Para obter mais informações, consulte Ações, recursos e chaves de condição do Route 53 Domains na Referência de autorização do serviço e Permissões de exemplo para um proprietário de registro de domínio.

Nomes de domínio internacionalizados

Com suporte para japonês.

Código de autorização necessário para transferir para o Route 53

Sim.

É necessário código de autorização para transferir para o Route 53

Sim.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: de 30 a 7 dias antes da data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 6 dias antes da validade
- A restauração com o registro é possível: entre em contato com o AWS Support.
- O domínio é excluído do registro: entre em contato com o AWS Support.

> **Note**
>
> No momento, não é possível registrar domínios do non-general-purpose Japão, como .co.jp e .or.jp.

.io (Território Britânico do Oceano Índico)

Ela também é usada como um TLD genérico, frequentemente por organizações relacionadas a computadores, como serviços online, jogos baseados em navegador e startups.

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Todas as informações são ocultas, exceto estado/província e país.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

O registro de domínios .io também usa o código de autorização como uma senha de uso único para algumas operações, como ativação ou desativação da proteção de privacidade. É necessário ter uma senha se você quiser executar mais de uma operação. Caso contrário, precisará gerar um novo código de autorização para cada operação.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 90 dias após a expiração

.net.au (Austrália)

Return to index

E-mail de confirmação do registro do TLD

Nosso associado registrador, Gandi, revende domínios.net.au por meio de. DomainDirectors Quando você transfere um nome de domínio para o Route 53, DomainDirectors envia um e-mail para o contato do registrante do domínio para verificar as informações de contato ou autorizar solicitações de transferência.

Período de contrato para registro e renovação

De 1 a 5 anos.

Restrições

Somente domínios de segundo nível estão disponíveis. O Route 53 oferece suporte aos domínios de segundo nível .com.au e net.au.

Aberto ao público, com algumas restrições:

- Os domínios .com.au e .net.au são abertos para empresas, comércio, parcerias ou comerciantes registrados na Austrália, para empresas estrangeiras licenciadas para praticar atividades comerciais na Austrália e para proprietários ou requerentes de uma marca registrada da Austrália.
- Seu nome de domínio deve ser idêntico ao seu nome, como registrado junto às autoridades australianas relevantes, ou à sua marca comercial (ou à abreviação ou acrônimo dela).
- O nome de domínio deve indicar sua atividade. Por exemplo, ele deve indicar um produto que você vende ou um serviço que fornece.
- Durante o processo de registro, você deve indicar o seguinte:
  - Seu tipo de registro: ABN (Número de registro comercial australiano), ACN (Número de empresa australiana) ou TM (Marca comercial) se o nome do domínio corresponder à sua marca comercial.
  - Seu número de ID: que pode ser um número de registro comercial australiano (ABN), um número de empresa australiana (ACN) ou a sua marca comercial (TM) se o nome do domínio corresponder à sua marca comercial.
  - Seu estado ou província.
- Informações de contato incorretas ou incompatíveis, incluindo nome, ABN ou número de marca comercial (TM) resultarão em falhas de registro, comércio e renovações. Uma alteração de propriedade pode ser necessária para corrigir informações para domínios existentes.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Ao definir a chave, você deve escolher o algoritmo de segurança DNS 2 (DH). Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 60 dias antes da expiração e a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 29 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 30 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .net.au não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

Como alterar uma propriedade

Altere o proprietário de modo programático ou com o console do Route 53. Consulte Atualizar informações de contato de um domínio. Em seguida, conclua o seguinte processo para concluir a alteração da propriedade:

1. Tanto os inscritos antigos quanto os novos devem clicar no link que receberam em um e-mail de transfers@1api.net para os endereços de e-mail listados. Se isso não for concluído em até 14 dias, terá de recomeçar o processo.

2. Após a confirmação das respostas, a alteração do proprietário no registro será processada em pouco tempo sem confirmação adicional.

.net.nz (Nova Zelândia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Você pode registrar os seguintes domínios de segundo nível com o Route 53: .co.nz, .net.nz e .org.nz. Não é possível registrar domínios .nz (primeiro nível) com o Route 53 nem transferi-los para o Route 53.

Aberto ao público, com algumas restrições:

- Os indivíduos devem ter, pelo menos, 18 anos.
- As organizações devem ser registradas.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 44 dias após a validade
- A restauração com o registro é possível: de 44 a 134 dias após a expiração
- O domínio é excluído do registro: 134 dias após a expiração

.org.nz (Nova Zelândia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Você pode registrar os seguintes domínios de segundo nível com o Route 53: .co.nz, .net.nz e .org.nz. Não é possível registrar domínios .nz (primeiro nível) com o Route 53 nem transferi-los para o Route 53.

Aberto ao público, com algumas restrições:

- Os indivíduos devem ter, pelo menos, 18 anos.
- As organizações devem ser registradas.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade

- O domínio é excluído do Route 53: 44 dias após a validade
- A restauração com o registro é possível: de 44 a 134 dias após a expiração
- O domínio é excluído do registro: 134 dias após a expiração

.pw (Palau)

Return to index

O .pw foi originalmente reservado para os residentes de Palau, um país insular na sub-região da Oceania, na Micronésia, no oeste do Pacífico, no entanto, agora é comumente usado para representar a “Web Profissional” e está disponível para todos.

Período de contrato para registro e renovação

De 1 a 10 anos.

Proteção de privacidade (aplica-se a todos os tipos de contato: pessoa, empresa, associação e órgão público)

Todas as informações ficam ocultas, exceto o nome da organização.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade

- O domínio é excluído do registro: 75 dias após a validade

.qa (Catar)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .qa ou transferir domínios .qa para o Route 53. Continuaremos a oferecer suporte a domínios .qa que já estão registrados no Route 53.

Return to index

Período de renovação

De 1 a 5 anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .qa para o Route 53.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: não

- O domínio é excluído do registro: 31 dias após a expiração

.ru (Federação Russa)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .ru ou transferir domínios .ru para o Route 53. Continuaremos a oferecer suporte a domínios .ru que já estão registrados no Route 53.

Return to index

Período de contrato para registro e renovação

1 ano.

> **Note**
>
> O registro de domínios.ru atualiza a data de expiração de um domínio no dia em que o domínio expira. Consultas WHOIS mostrarão a data de validade antiga do domínio até essa data, independentemente de quando você renovar o domínio com o Route 53.

Restrições

Aberto ao público, com algumas restrições:

- Os indivíduos podem precisar fornecer o número do passaporte ou de um documento de identidade emitido pelo governo.
- As empresas estrangeiras podem precisar fornecer um ID ou um registro da empresa.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do

Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .ru para o Route 53.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até 2 dias antes da data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 2 dias antes da validade
- A restauração com o registro é possível: entre 2 dias antes e 28 dias após a expiração
- O domínio é excluído do registro: 28 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .ru não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.sg (República de Singapura)

> **Important**
>
> Você não pode mais usar o Route 53 para registrar novos domínios .sg ou transferir domínios .sg para o Route 53. Continuaremos a oferecer suporte a domínios .sg que já estão registrados no Route 53.

Return to index

Período de renovação

Um ou dois anos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Código de autorização necessário para transferir para o Route 53

Sem suporte. Não é mais possível transferir domínios .sg para o Route 53.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 60 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .sg não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

Europa

É possível usar os domínios de nível superior (TLDs) a seguir para a Europa com o objetivo de registrar domínios no Amazon Route 53.

, , , , , , , , , , , , , , , , , , , ,

Return to index

.be (Bélgica)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim. Você pode obter o código de transferência no site da DNS Belgium.

É necessário código de autorização para transferir para o Route 53

Sim. Você pode obter o código de transferência no site da DNS Belgium.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: na data de validade
- A restauração com o registro é possível: até 40 dias após a expiração
- O domínio é excluído do registro: 40 dias após a expiração

.berlin (cidade de Berlim na Alemanha)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com algumas restrições:

- O proprietário, o contato administrativo ou técnico deve fornecer um endereço em Berlim e o contato administrativo deve ser um indivíduo.
- Você deverá ativar e usar seu domínio .berlin em até 12 meses após seu registro (aplicável a um site, redirecionamento ou endereço de e-mail).
- Se você publicar um site em seu domínio .berlin ou se o domínio redirecionar para outro site, o conteúdo do site deverá ser relacionado a Berlim.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para latim e cirílico.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 80 dias após a validade

.ch (Suíça)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 9 dias após a validade
- O domínio é excluído do Route 53: 9 dias após a validade
- A restauração com o registro é possível: entre 9 e 49 dias após a expiração
- O domínio é excluído do registro: 49 dias após a expiração

.co.uk (Reino Unido)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Se você estiver transferindo um domínio .co.uk para o Route 53, não será necessário obter um código de autorização. Em vez disso, use o método fornecido pelo registrador de domínio atual para atualizar o valor da tag de IPS do domínio para GANDI, tudo em letras maiúsculas. (Uma tag de IPS é exigida pelo Nominet, entidade responsável pela gestão dos domínios .uk.) Se o seu registrador não alterar o valor da tag de IPS, entre em contato com o Nominet.

> **Note**
>
> Quando você registra um domínio .co.uk, o Route 53 define automaticamente a tag IPS do domínio como GANDI.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 180 dias antes e 30 dias após a data de expiração

- A renovação tardia com o Route 53 é possível: entre 30 e 90 dias após a validade
- O domínio é excluído do Route 53: 90 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 92 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .co.uk não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.cz (República Tcheca)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Não há suporte, mas o endereço de e-mail e o número de telefone estão ocultos para todos os contatos.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

Se o registrador atual não fornecer um código de autorização, acesse `https://www.nic.cz/whois/send-password/` para solicitar que ele seja enviado ao endereço de e-mail do registrante pelo registro de domínio CZ.

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 58 dias após a validade
- O domínio é excluído do Route 53: 59 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 60 dias após a expiração

.de (Alemanha)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, com algumas restrições:

- Você deve residir na Alemanha ou ter um contato administrativo (pessoa física) que resida na Alemanha e tenha um endereço que não seja uma caixa postal.
- Durante o registro, o DNS (A, MX e CNAME) do nome de domínio deve ser configurado corretamente para passar pela verificação da zona do registro. São necessários três servidores de duas classes C diferentes.
- Se você estiver usando um serviço DNS diferente do Route 53, os servidores de nomes do domínio deverão passar por uma verificação para garantir que eles estejam configurados corretamente. Para determinar se os servidores de nome do seu domínio passarão na verificação, consulte https://www.denic.de/en/service/tools/nast/.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do

Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: na data de validade
- A restauração com o registro é possível: entre em contato com o AWS Support.
- O domínio é excluído do registro: entre em contato com o AWS Support.

.es (Espanha)

Return to index

Compra ou transferência de domínio

> **Important**
>
> No momento, você pode comprar novos nomes de domínio .es ou transferir domínios .es para o Route 53, se o tipo de contato do registrante for Person (Pessoa). Não é possível comprar ou transferir domínios .es, se o tipo de contato do registrante for Empresa, Associação ou Órgão público.
> Você também não pode alterar o tipo de contato do registrante para Empresa.

Período de contrato para registro e renovação

De 1 a 5 anos.

Restrições

Aberto ao público, para quem tem interesse na Espanha ou uma conexão com esse país.

A partir de 2016, os registrantes do domínio .ES devem fornecer um e-mail de contato do registrante. Se você ainda não forneceu essa informação, precisará fazê-lo no registrador atual antes de transferir seu domínio para o Route 53.

Você precisará das seguintes informações:

- Identificador do ESNIC semelhante a *AAAA0-ESNIC-F0*.
- Se você não souber seu identificador do ESNIC, poderá obtê-lo com o registrador atual. Você pode encontrar o registrador em: https://www.dominios.es/en.

Dependendo de se lembrar ou não de sua senha no registrador, você poderá seguir um dos seguintes procedimentos para atualizar seu e-mail de registrante:

- Se você se lembrar de sua senha, faça login em https://www.nic.es/sgnd/login.action usando seu identificador e sua senha do ESNIC.

  Depois de fazer login, você pode editar o e-mail para contato do registrante escolhendo a guia Edit na página do registro.
- Se você esqueceu sua senha, navegue até https://www.nic.es/sgnd/peticion/editCorreo.action?request_locale=en.

  Preencha o formulário com seu identificador do ESNIC e seu novo contato de e-mail de registrante válido. Depois, valide o formulário escolhendo Processing without eID/Certificate e carregue o documento de identidade solicitado.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Para evitar transferências não autorizadas, restrinja o acesso ao endereço de e-mail do registrante e às APIs do Route 53 que poderiam permitir a mudança de propriedade, por exemplo, Contato. UpdateDomain Para obter mais informações, consulte Ações, recursos e chaves de condição do Route 53 Domains na Referência de autorização do serviço e Permissões de exemplo para um proprietário de registro de domínio.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Não

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até 6 dias antes da data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 6 dias antes da validade
- A restauração com o registro é possível: entre 6 dias antes e 4 dias após a expiração
- O domínio é excluído do registro: 4 dias após a expiração

.eu (União Europeia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com uma restrição:

- Você deve fornecer um endereço postal válido de um dos 30 estados do Espaço Econômico Europeu (EEE) ou, se for cidadão de um dos 27 Estados-Membros da União Europeia (UE), deve especificar o seu país de cidadania da UE.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: na data de validade
- A restauração com o registro é possível: até 40 dias após a expiração
- O domínio é excluído do registro: 40 dias após a expiração

Pesquisa WHOIS

Para obter informações sobre domínios .eu existentes, consulte https://whois.eurid.eu/en/.

.fi (Finlândia)

Return to index

Período de contrato para registro e renovação

De 1 a 5 anos.

Restrições

Aberto ao público, com algumas restrições:

- A extensão .fi está disponível para indivíduos com domicílio na Finlândia e um número de identidade finlandês, além de empresas (inclusive da iniciativa privada) registradas na Finlândia.
- Se o endereço de contato do registrante estiver na Finlândia, o número de identidade finlandês será necessário para um registrante individual e o número da empresa finlandesa será necessário para o registrante da empresa, e você deve fornecer as seguintes informações durante o registro:

- Se o contato é baseado ou não em uma pessoa física ou idônea na Finlândia.
- O identificador do registro em que o nome é registrado, se for baseado no nome de uma pessoa idônea.
- O número do registro em que o nome é registrado, se for baseado no nome de uma pessoa idônea.
- O número de identificação de uma pessoa idônea na Finlândia.
- O número de identificação de uma pessoa física na Finlândia.
- Se o registrante for uma empresa não finlandesa, você deverá fornecer o número comercial como número de IVA.

- Se o endereço do registrante não estiver localizado na Finlândia, não será necessário nenhum número de identidade ou empresa finlandês.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade

- A restauração com o registro é possível: não
- O domínio é excluído do registro: não

Exclusão de registro de domínio

Para obter informações sobre como excluir domínios, consulte Excluir um registro de nome de domínio.

.fr (França)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com algumas restrições:

- Os indivíduos devem ter, no mínimo, 18 anos e informar sua data de nascimento.
- As organizações devem estar localizadas na Área Econômica Europeia ou na Suíça.
- As organizações devem preencher todos os campos de identificação da empresa (número de IVA, SIREN, WALDEC, DUNS e assim por diante), pois isso facilitará as verificações que a AFNIC poderá realizar posteriormente.
- As mesmas condições de qualificação se aplicam ao contato administrativo.
- Os nomes e os termos estão sujeitos a uma revisão prévia da AFNIC (Carta de nomeação, artigo 2.4) e às seguintes condições adicionais:
  - Os nomes de domínio antes reservados ou proibidos são abertos a candidatos que justificarem um direito legítimo e agirem de boa-fé.
  - Os nomes que começam com ville, mairie, agglo, cc, cg e cr estão sujeitos às convenções de nomenclatura da AFNIC.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 27 dias após a validade
- O domínio é excluído do Route 53: 28 dias após a validade
- A restauração com o registro é possível: entre 28 e 58 dias após a expiração
- O domínio é excluído do registro: 58 dias após a expiração

.gg (Guernsey)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 35 dias após a expiração
- O domínio é excluído do registro: 35 dias após a expiração

.im (Ilha de Man)

Ela também é usada como um TLD genérico, frequentemente por serviços de mensagens instantâneas ou indivíduos que desejam desenvolver uma marca pessoal "Eu sou".

Return to index

Período de contrato para registro e renovação

Um ou dois anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 30 dias após a expiração

.it (Itália)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, com algumas restrições:

- Os indivíduos ou as organizações devem ter um endereço registrado na União Europeia.
- Se o seu país de origem é a Itália, você deve inserir um código fiscal. Se o seu país de origem fica na União Europeia, você deve inserir o número do documento de identidade (número do ID).
- Se você especificar Empresa, Associação ou Órgão público como tipo de contato, será necessário informar um número de IVA (número de identificação fiscal de valor agregado).
- Os servidores de nome do seu domínio devem passar por uma verificação de DNS. Sugerimos que você verifique os servidores de nomes em https://dns-check.nic.it/ antes de enviar a solicitação de alteração. Se o nome do seu domínio não estiver em conformidade com os requisitos técnicos (por exemplo, não estiver associado a um nome de servidor operacional) e não for corrigido em até 30 dias, ele será excluído pelo registro. Nós não emitimos reembolsos para domínios que são excluídos porque não atendem aos requisitos técnicos.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Compatível.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Sem suporte.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 13 dias após a validade
- O domínio é excluído do registro: 49 dias após a expiração
- A restauração com o registro é possível: entre 14 e 44 dias após a expiração
- O domínio é excluído do registro: entre em contato com o AWS Support.

.me (Montenegro)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Domain.me, o registro de domínios .me, considera nomes de domínio de duas letras e alguns nomes de domínio mais longos como nomes de domínio premium. Não é possível registrar

domínios .me premium no Route 53 ou transferi-los para ele. Para obter mais informações sobre nomes de domínio .me premium, consulte o site domain.me.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para árabe, bielorrusso, bósnio, búlgaro, chinês simplificado, chinês tradicional, croata, dinamarquês, francês, alemão, hindi, húngaro, islandês, italiano, coreano, letão, lituano, mongol, montenegrino, polonês, português, russo, sérvio, espanhol, sueco, turco e ucraniano.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 29 dias após a validade
- O domínio é excluído do Route 53: 30 dias após a validade
- A restauração com o registro é possível: entre 30 e 60 dias após a expiração
- O domínio é excluído do registro: 65 dias após a expiração

.me.uk (Reino Unido)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Se você estiver transferindo um domínio .me.uk para o Route 53, não será necessário obter um código de autorização. Em vez disso, use o método fornecido pelo registrador de domínio atual para atualizar o valor da tag de IPS do domínio para GANDI, tudo em letras maiúsculas. (Uma tag de IPS é exigida pelo Nominet, entidade responsável pela gestão dos domínios .uk.) Se o seu registrador não alterar o valor da tag de IPS, entre em contato com o Nominet.

> **Note**
>
> Quando você registra um domínio .me.uk, o Route 53 define automaticamente a tag IPS do domínio como GANDI.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 180 dias antes e 30 dias após a data de expiração
- A renovação tardia com o Route 53 é possível: entre 30 e 90 dias após a validade
- O domínio é excluído do Route 53: 90 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 92 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .me.uk não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.nl (Holanda)

Return to index

Período de contrato para registro e renovação

1 ano.

Restrições

Aberto ao público, com algumas restrições:

- O proprietário ou o contato administrativo deve fornecer um endereço válido na Holanda. Uma presença local é obrigatória.
- Se você não tiver um endereço válido na Holanda, o SIDN de registros fornecerá um endereço domiciliar, de acordo com o Procedimento de endereço domiciliar.
- O nome de domínio deve ter 3-63 caracteres, excluindo .nl.

Proteção da privacidade

Determinada pelo registro.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até 1 dia antes da data de expiração

- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 1 dia antes da validade
- A restauração com o registro é possível: entre 1 dia antes e 39 dias após a expiração
- O domínio é excluído do registro: 39 dias após a expiração

.org.uk (Reino Unido)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Se você estiver transferindo um domínio .org.uk para o Route 53, não será necessário obter um código de autorização. Em vez disso, use o método fornecido pelo registrador de domínio atual para atualizar o valor da tag de IPS do domínio para GANDI, tudo em letras maiúsculas. (Uma tag de IPS é exigida pelo Nominet, entidade responsável pela gestão dos domínios .uk.) Se o seu registrador não alterar o valor da tag de IPS, entre em contato com o Nominet.

> **Note**
>
> Quando você registra um domínio .org.uk, o Route 53 define automaticamente a tag IPS do domínio como GANDI.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 180 dias antes e 30 dias após a data de expiração
- A renovação tardia com o Route 53 é possível: entre 30 e 90 dias após a validade
- O domínio é excluído do Route 53: 90 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 92 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .org.uk não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.ruhr (região de Ruhr, parte ocidental da Alemanha)

Return to index

A extensão .ruhr é destinada à região de Ruhr (parte ocidental da Alemanha).

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com uma restrição:

- O contato administrativo deve ser um indivíduo com um endereço na Alemanha.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte (ä, ö, ü, ß).

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: entre em contato com o AWS Support.

.se (Suécia)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com algumas restrições:

- Se você está na Suécia, deve fornecer um número de ID sueco válido. O formato do número de identificação é`YYMMDD-NNNN`.
- Se você está fora da Suécia, deve inserir um número de ID válido, como um número de ID fiscal.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Sem suporte. Recomendamos que você evite transferências não autorizadas restringindo o acesso à ação da RetrieveDomainAuthCodeAPI. (Ao restringir o acesso a essa API do Route 53, você também restringe quem pode gerar um código de autorização usando o console do

Route 53, AWS SDKs e outros métodos programáticos.) Para ter mais informações, consulte Gerenciamento de identidade e acesso no Amazon Route 53.

Nomes de domínio internacionalizados

Com suporte para latim, sueco e ídiche.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até 1 dia antes da data de expiração
- A renovação tardia com o Route 53 é possível: não
- O domínio é excluído do Route 53: 1 dia antes da validade
- A restauração com o registro é possível: entre 1 dia antes e 59 dias após a expiração
- O domínio é excluído do registro: 64 dias após a expiração

.uk (Reino Unido)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, sem restrições.

Proteção da privacidade

Todas as informações são ocultas.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível

Nomes de domínio internacionalizados

Sem suporte.

Código de autorização necessário para transferir para o Route 53

Se você estiver transferindo um domínio uk para o Route 53, não será necessário obter um código de autorização. Em vez disso, use o método fornecido pelo registrador de domínio atual para atualizar o valor da tag de IPS do domínio para GANDI, tudo em letras maiúsculas. (Uma tag de IPS é exigida pelo Nominet, entidade responsável pela gestão dos domínios .uk.) Se o seu registrador não alterar o valor da tag de IPS, entre em contato com o Nominet.

> **Note**
>
> Quando você registra um domínio .uk, o Route 53 define automaticamente a tag de IPS do domínio como GANDI.

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: entre 180 dias antes e 30 dias após a data de expiração
- A renovação tardia com o Route 53 é possível: entre 30 e 90 dias após a validade
- O domínio é excluído do Route 53: 90 dias após a validade
- A restauração com o registro é possível: não
- O domínio é excluído do registro: 92 dias após a expiração

Exclusão de registro de domínio

O registro de domínios .uk não permite que você exclua registros de domínio. Em vez disso, você deve desativar a renovação automática e esperar que o domínio expire. Para ter mais informações, consulte Excluir um registro de nome de domínio.

.wien (cidade de Viena, na Áustria)

Return to index

Período de contrato para registro e renovação

De 1 a 10 anos.

Restrições

Aberto ao público, com algumas restrições:

- Você deve mostrar uma afinidade econômica, cultural, turística, histórica, social ou outra afinidade com a cidade de Viena, na Áustria.
- Os nomes de domínio .wien devem ser usados em conjunto com as condições acima durante todo o período de vigência do registro.

Proteção da privacidade

Sem suporte.

Bloqueio de domínio para impedir transferências não autorizadas

Compatível.

Nomes de domínio internacionalizados

Com suporte para latim.

Código de autorização necessário para transferir para o Route 53

Sim

DNSSEC

Com suporte para registro de domínio. Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

Prazos para renovação e restauração de domínios

- A renovação é possível: até a data de expiração
- A renovação tardia com o Route 53 é possível: até 44 dias após a validade
- O domínio é excluído do Route 53: 45 dias após a validade
- A restauração com o registro é possível: entre 45 e 75 dias após a validade
- O domínio é excluído do registro: 80 dias após a validade

Configurar o Amazon Route 53 como serviço DNS

Você pode usar o Amazon Route 53 como o serviço DNS para seu domínio, como example.com. Quando o Route 53 for o seu serviço DNS, ele encaminhará o tráfego da Internet para o seu site convertendo nomes de domínio amigáveis, como www.example.com, em endereços IP numéricos, como 192.0.2.1, que os computadores usam para se conectar uns aos outros. Quando alguém digita seu nome de domínio em um navegador ou envia um e-mail para você, uma consulta de DNS é encaminhada para o Route 53, que responde com o valor apropriado. Por exemplo, o Route 53 pode responder com o endereço IP para o servidor da Web para example.com.

Neste capítulo, explicaremos como configurar o Route 53 para encaminhar seu tráfego de Internet para locais apropriados. Também explicaremos como migrar o serviço DNS para o Route 53, se você estiver usando outro serviço DNS e como usar o Route 53 como o serviço DNS de um novo domínio.

Tópicos

Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente

Se você estiver transferindo um ou mais registros de domínio para o Route 53 e estiver usando um registrador de domínio que não forneça um serviço de DNS pago, será necessário migrar o serviço DNS antes de migrar o domínio. Caso contrário, o registrador deixará de fornecer serviços de DNS quando você transferir seus domínios, e os sites e aplicações Web associados ficarão indisponíveis na Internet. (Você também pode migrar o serviço de DNS do registrador atual para outro provedor de serviços de DNS. Nós não exigimos que você use o Route 53 como o provedor de serviços DNS para domínios registrados com o Route 53.)

O processo depende se você está usando o domínio na ocasião:

- Se o domínio estiver recebendo tráfego atualmente, por exemplo, se os usuários estiverem usando o nome de domínio para navegar em um site ou acessar uma aplicação Web, consulte Tornar o Route 53 o serviço de DNS para um domínio que está em uso.
- Se o domínio não estiver recebendo nenhum tráfego (ou recebendo pouquíssimo tráfego), consulte Tornar o Route 53 o serviço DNS para um domínio inativo.

Em ambas as opções, seu domínio deve permanecer disponível durante todo o processo de migração. No entanto, no caso improvável de ocorrer algum problema, a primeira opção permite reverter a migração rapidamente. Com a segunda opção, seu domínio pode ficar indisponível para alguns dias.

Se você quiser entrar em contato com um especialista em AWS, visite o suporte de vendas.

Tornar o Route 53 o serviço de DNS para um domínio que está em uso

Se quiser migrar o serviço DNS para o Amazon Route 53 para um domínio que atualmente está recebendo tráfego, por exemplo, se os usuários estiverem usando o nome de domínio para navegar em um site ou acessar uma aplicação Web, execute os procedimentos desta seção.

Tópicos

Etapa 1: descobrir a configuração atual do DNS com o provedor de serviço de DNS atual (opcional, mas recomendado)

Ao migrar o serviço DNS de outro provedor para o Route 53, você reproduz a configuração DNS atual no Route 53. No Route 53, você cria uma zona hospedada que tem o mesmo nome que seu domínio e cria registros nela. Cada registro indica como você deseja direcionar o tráfego para um nome de domínio ou nome de subdomínio especificado. Por exemplo, quando alguém insere o nome de seu domínio em um navegador da Web, você deseja que o tráfego seja encaminhado para um servidor Web em seu datacenter, para uma instância do Amazon EC2, para uma distribuição do CloudFront ou para algum outro local?

O processo usado depende da complexidade da sua configuração DNS atual:

- Se sua configuração DNS atual for simples: se você estiver encaminhando o tráfego da Internet de apenas alguns subdomínios para um pequeno número de recursos, como servidores Web ou buckets do Amazon S3, você poderá criar alguns registros manualmente no console do Route 53.
- Se sua configuração DNS atual for mais complexa e você quiser apenas reproduzir a configuração atual: você poderá simplificar a migração se puder obter um arquivo de zona do provedor de serviço DNS atual e importar o arquivo de zona no Route 53. (Nem todos os provedores de serviço de DNS disponibilizam os arquivos de zona.) Quando você importa um arquivo de zona, o Route 53 reproduz automaticamente a configuração existente, criando os registros correspondentes em sua zona hospedada.

  Entre em contato com o suporte ao cliente do atual provedor de serviço de DNS para obter um arquivo de zona ou uma lista de registros. Para mais informações sobre o formato exigido do arquivo de zona, consulte Criar registros importando um arquivo de zona.
- Se a sua configuração DNS atual for mais complexa, e você estiver interessado nos recursos de roteamento do Route 53: analise a documentação a seguir para ver se deseja usar os recursos do Route 53 que não estão disponíveis em outros provedores de serviço DNS. Se for o caso, você pode criar registros manualmente ou pode importar um arquivo de zona e, em seguida, criar ou atualizar registros posteriormente:
  - Escolher entre registros de alias e não alias explica as vantagens de registros com alias do Route 53, que encaminham o tráfego para alguns recursos da AWS, como distribuições do CloudFront e buckets do Amazon S3, gratuitamente.
  - A Escolher uma política de roteamento explica as opções de roteamento do Route 53, por exemplo, roteamento com base na localização de seus usuários, roteamento com base na

latência entre seus usuários e seus recursos, roteamento com base na integridade de seus recursos e roteamento para recursos com base em ponderações especificadas por você.

> **Note**
>
> Você também pode importar um arquivo de zona e depois alterar sua configuração de aproveitar os registros de alias e as políticas de roteamento complexas.

Se não for possível obter um arquivo de zona ou se você quiser criar registros manualmente no Route 53, os registros que você vai migrar incluirão o seguinte:

- A (Address) records (Registros A (Endereço): associam um nome de domínio ou um nome de subdomínio ao endereço IPv4 (por exemplo, 192.0.2.3) do recurso correspondente
- AAAA (Address) records (Registros AAAA (Endereço): associam um nome de domínio ou um nome de subdomínio ao endereço IPv6 (por exemplo, 2001:0db8:85a3:0000:0000:abcd:0001:2345) do recurso correspondente
- Mail server (MX) records (Registros de servidor de e-mail (MX): encaminham tráfego para os servidores de e-mail
- CNAME records (Registros CNAME): reencaminham o tráfego de um nome de domínio (exemplo.net) para outro nome de domínio (exemplo.com)
- Records for other supported DNS record types (Registros de outros tipos de registros DNS compatíveis): para obter uma lista de tipos de registros compatíveis, consulte Tipos de registro de DNS com suporte.

Etapa 2: criar uma zona hospedada

Para informar ao Amazon Route 53 como você quer encaminhar o tráfego para seu domínio, crie uma zona hospedada com o mesmo nome que o seu domínio e, em seguida, crie registros nela.

> **Important**
>
> Você pode criar uma zona hospedada somente para um domínio que você tenha permissão para administrar. Normalmente, isso significa que você tem o domínio, mas também pode estar desenvolvendo uma aplicação para o proprietário dele.

Quando você cria uma zona hospedada, o Route 53 cria automaticamente um registro de servidor de nome (NS) e de início de autoridade (SOA) para a zona. O registro NS identifica os quatro servidores de nome que o Route 53 associou à sua zona hospedada. Para tornar o Route 53 o serviço de DNS do seu domínio, atualize o registro do domínio para usar esses quatro servidores de nome.

> **Important**
>
> Não crie registros adicionais de NS (servidor de nome) ou SOA (início de autoridade) e não exclua os registros de NS e SOA existentes.

Para criar uma zona hospedada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Se você for novo no Route 53, escolha Get started (Conceitos básicos) em DNS management (Gerenciamento de DNS) e, depois, escolha Create hosted zones (Criar zonas hospedadas).

   Se já estiver usando o Route 53, escolha Hosted zones (Zonas hospedadas) no painel de navegação e escolha Create hosted zones (Criar zonas hospedadas).
3. No painel Create hosted zone (Criar zona hospedada), insira um nome de domínio e, se preferir, um comentário. Para obter mais informações sobre uma configuração, escolha abrir o painel de ajuda no lado direito.

   Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.
4. Para Type (Tipo), aceite o valor padrão da Public hosted zone (Zona pública hospedada).
5. Escolha Create hosted zone (Criar zona hospedada).

Etapa 3: criar registros

Depois de criar uma zona hospedada, crie registros na zona hospedada que define onde você deseja redirecionar o tráfego para um domínio (exemplo.com) ou subdomínio (www.exemplo.com). Por exemplo, se você deseja encaminhar o tráfego para exemplo.com e www.exemplo.com para um servidor Web em uma instância do Amazon EC2, crie dois registros, um chamado exemplo.com e o

outro chamado www.exemplo.com. Em cada registro, especifique o endereço IP para sua instância do EC2.

Você pode criar registros em uma série de formas:

Importar um arquivo de zona

Este é o método mais fácil se você tiver um arquivo de zona do seu serviço de DNS atual em Etapa 1: descobrir a configuração atual do DNS com o provedor de serviço de DNS atual (opcional, mas recomendado). O Amazon Route 53 não prevê quando deve criar registros de alias ou usar tipos de roteamento especiais, como ponderado ou failover. Como resultado, se você importar um arquivo de zona, o Route 53 cria registros de DNS padrão usando a política de roteamento simples.

Para obter mais informações, consulte Criar registros importando um arquivo de zona.

Criar registros individualmente no console

Se você não obteve o arquivo de zona e apenas deseja criar alguns registros com uma política de roteamento Simples para começar, você pode criar os registros no console do Route 53. Você pode criar registros com alias e sem alias.

Para mais informações, consulte os tópicos a seguir:

- Escolher uma política de roteamento
- Escolher entre registros de alias e não alias
- Criar registros usando o console do Amazon Route 53

Criar registros de forma programática

Você pode criar registros usando um dos SDKs, a AWS CLI ou o AWS Tools for Windows PowerShell da AWS. Para obter mais informações, consulte a Documentação do AWS.

Se você estiver usando uma linguagem de programação para a qual a AWS não fornece um SDK, você também pode usar a API do Route 53. Para obter mais informações, consulte Referência de API do Amazon Route 53.

Etapa 4: reduzir as configurações de TTL

A configuração de TTL (vida útil) de um registro especifica por quanto tempo você deseja que os resolvedores de DNS armazenem o registro e usem as informações em cache. Quando o TTL expira,

um resolvedor envia outra consulta para o provedor de serviço de DNS para um domínio a fim de obter as informações mais recentes.

A configuração de TTL típica para o registro de NS é de 172.800 segundos, ou dois dias. O registro de NS lista os servidores de nome que o Sistema de Nomes de Domínio (DNS) pode usar para obter informações sobre como direcionar o tráfego para o seu domínio. Reduzir o TTL do registro de NS, tanto no provedor de serviço DNS atual quanto no Amazon Route 53, reduz o tempo de inatividade do seu domínio quando você descobre um problema durante a migração do DNS para o Route 53. Se você não reduzir o TTL, seu domínio pode ficar indisponível na Internet por até dois dias se algo der errado.

> **Note**
>
> Alguns resolvedores completos podem armazenar em cache o TTL do registro de NS do servidor superior confiável, portanto, o TTL dos registros de NS registrados no servidor DNS confiável também deve ser reduzido.

Recomendamos que você altere o TTL nos seguintes registros de NS:

- No registro de NS na zona hospedada para o provedor de serviço de DNS atual. (O provedor atual pode usar uma terminologia diferente.)
- No registro de NS na zona hospedada que você criou em Etapa 2: criar uma zona hospedada.

Para reduzir a configuração de TTL no registro de NS com o provedor de serviço de DNS atual

- Use o método fornecido pelo provedor de serviço de DNS atual para o domínio a fim de alterar o TTL para o registro de NS na zona hospedada de seu domínio.

Para reduzir a configuração de TTL no registro de NS em uma zona hospedada do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Escolha Hosted Zones (Zonas hospedadas) no painel de navegação.
3. Escolha o nome da zona hospedada.
4. Escolha o registro de NS e escolha Edit (Editar).

5. Altere o valor de TTL (Seconds) (TTL [segundos]). Recomendamos que você especifique um valor entre 60 segundos e 900 segundos (15 minutos).
6. Selecione Save changes (Salvar alterações).

Etapa 5: (Se você tiver o DNSSEC configurado) Remova o registro DS da zona pai

Se você configurou o DNSSEC para seu domínio, remova o registro DS (Delegation Signer) da zona pai antes de migrar seu domínio para o Route 53.

Caso a zona pai esteja hospedada por meio do Route 53 ou de outro registrador, entre em contato com eles para remover o registro DS.

Como atualmente não é possível ter a assinatura de DNSSEC habilitada em dois provedores, é necessário remover qualquer DS ou DNSSEYs para desativar o DNSSEC. Isso é sinalizado temporariamente para os resolvedores DNS para desabilitar a validação DNSSEC. Na etapa 11, você poderá reabilitar a validação DNSSEC, se desejar, após a conclusão da transição para o Route 53.

Para obter mais informações, consulte Excluir chaves públicas de um domínio.

Etapa 6: Aguardar pela expiração do TTL antigo

Se seu domínio estiver em uso, por exemplo, se os usuários estiverem usando o nome de domínio para navegar em um site ou acessar uma aplicação Web, os resolvedores DNS terão armazenado em cache os nomes dos servidores de nomes que foram fornecidos por seu provedor de serviço DNS atual. Um resolvedor de DNS que armazenou essas informações em cache alguns minutos atrás irá salvá-los por quase dois dias adicionais.

Para garantir que a migração do serviço de DNS para o Route 53 aconteça de uma vez só, aguarde dois dias após reduzir o TTL. Após o TTL de dois dias expirar e os resolvedores solicitarem os servidores de nome para o seu domínio, os resolvedores receberão os servidores de nome atuais e também o novo TTL que você especificou em Etapa 4: reduzir as configurações de TTL.

Etapa 7: Atualizar os registros NS para usar servidores de nome do Route 53

Para começar a usar o Amazon Route 53 como o serviço DNS para um domínio, use o método fornecido pelo registrador, ou pela zona pai, para substituir os servidores de nomes atuais no registro NS por servidores de nomes do Route 53.

> **Note**
>
> Ao atualizar o registro NS com o provedor atual de serviços DNS para usar servidores de nomes do Route 53, você está atualizando a configuração de DNS para o domínio. (Isso é comparável a atualizar o registro de NS na zona hospedada do Route 53 para um domínio, exceto que você está atualizando a configuração com o serviço DNS do qual você está migrando.)

Para atualizar o registro NS no registrador ou na zona pai, use os servidores de nome do Route 53

1. No console do Route 53, obtenha os servidores de nomes de sua zona hospedada:
   a. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
   b. No painel de navegação, escolha Zonas hospedadas.
   c. Na página Hosted zones (Zonas hospedadas), escolha o nome para a zona hospedada aplicável.
   d. Anote os quatro nomes listados para Name servers (Servidores de nome) na seção Hosted zone details (Detalhes da zona hospedada).
2. Use o método que é fornecido pelo serviço de DNS atual para o domínio, a fim de atualizar o registro de NS para a zona hospedada. Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio. O processo vai depender se o serviço de DNS atual permitir ou não que você exclua os servidores de nome:

   Se você pode excluir os servidores de nome

   - Anote os nomes dos servidores de nome atuais no registro de NS da zona hospedada. Se precisar reverter para a configuração de DNS atual, esses são os servidores que você especificará.
   - Exclua os servidores de nome atuais do registro de NS.
   - Atualize o registro de NS com os nomes de todos os quatro servidores de nome do Route 53 que você obteve na etapa 1 deste procedimento.

> **Note**
>
> Quando você tiver terminado, os únicos servidores de nome no registro de NS serão os quatro servidores de nome do Route 53.

Se você não pode excluir os servidores de nome

- Escolha a opção para usar servidores de nome personalizados.
- Adicione todos os quatro servidores de nome do Route 53 que você obteve na etapa 1 deste procedimento.

Etapa 8: Monitorar o tráfego do domínio

Monitore o tráfego do domínio, incluindo o tráfego do site ou da aplicação e do e-mail:

- Se o tráfego diminuir ou for interrompido: use o método fornecido pelo serviço DNS anterior para alterar os servidores de nomes do domínio de volta para os servidores de nomes anteriores. Esses são os servidores de nome que você anotou na etapa 7 de Para atualizar o registro NS no registrador ou na zona pai, use os servidores de nome do Route 53. Em seguida, determine o que deu errado.
- Se o tráfego não for afetado: continue em Etapa 9: alterar o TTL para o registro de NS de volta para um valor maior.

Etapa 9: alterar o TTL para o registro de NS de volta para um valor maior

Na zona hospedada do Amazon Route 53 para o domínio, altere o TTL do registro de NS para um valor mais comum. Por exemplo, 172.800 segundos (dois dias). Isso melhora a latência para seus usuários, pois eles não precisam esperar que os resolvedores de DNS enviem uma consulta para os servidores de nome do seu domínio.

Para alterar o TTL para o registro de NS na zona hospedada do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Escolha Hosted Zones (Zonas hospedadas) no painel de navegação.

3. Escolha o nome da zona hospedada.
4. Na lista de registros da zona hospedada, escolha o registro de NS.
5. Selecione Edit (Editar).
6. Altere TTL (Seconds) (TTL [segundos]) para o número de segundos que você deseja que os resolvedores de DNS armazenem em cache os nomes dos servidores de nome do seu domínio. Recomendamos um valor de 172.800 segundos.
7. Escolha Save changes (Salvar alterações).

Etapa 10: Transferir o registro de um domínio para o Amazon Route 53

Agora que você transferiu o serviço DNS de um domínio para o Amazon Route 53, existe a opção de transferir o registro desse domínio para o Route 53. Para obter mais informações, consulte Como transferir registro de um domínio para o Amazon Route 53.

Etapa 11: Reabilite a assinatura de DNSSEC (se necessário)

Agora que você transferiu o serviço DNS de um domínio para o Amazon Route 53, é possível reabilitar a assinatura de DNSSEC.

A habilitação da assinatura de DNSSEC tem duas etapas:

- Etapa 1: Habilitar a assinatura de DNSSEC para o Route 53 e solicitar que o Route 53 crie uma chave de assinatura da chave (KSK) com base em uma chave gerenciada pelo cliente no AWS Key Management Service (AWS KMS).
- Etapa 2: Criar uma cadeia de confiança para a zona hospedada adicionando um registro DS (Delegation Signer) à zona pai, para que as respostas DNS possam ser autenticadas com assinaturas criptográficas confiáveis.

  Para obter instruções, consulte Como habilitar a assinatura de DNSSEC e estabelecer uma cadeia de confiança.

Tornar o Route 53 o serviço DNS para um domínio inativo

Se você quiser migrar o serviço de DNS do Amazon Route 53 para um domínio que não está recebendo nenhum tráfego (ou apresenta muito pouco tráfego), realize os procedimentos nesta seção.

Tópicos

Etapa 1: descobrir a configuração atual do DNS com o provedor de serviço de DNS atual (domínios inativos)

Ao migrar o serviço DNS de outro provedor para o Route 53, você reproduz a configuração DNS atual no Route 53. No Route 53, você cria uma zona hospedada que tem o mesmo nome que seu domínio e cria registros nela. Cada registro indica como você deseja direcionar o tráfego para um nome de domínio ou nome de subdomínio especificado. Por exemplo, quando alguém insere o nome de seu domínio em um navegador da Web, você deseja que o tráfego seja encaminhado para um servidor Web em seu datacenter, para uma instância do Amazon EC2, para uma distribuição do CloudFront ou para algum outro local?

O processo usado depende da complexidade da sua configuração DNS atual:

- Se sua configuração DNS atual for simples: se você estiver encaminhando o tráfego da Internet de apenas alguns subdomínios para um pequeno número de recursos, como servidores Web ou buckets do Amazon S3, você poderá criar alguns registros manualmente no console do Route 53.
- Se sua configuração DNS atual for mais complexa e você quiser apenas reproduzir a configuração atual: você poderá simplificar a migração se puder obter um arquivo de zona do provedor de serviço DNS atual e importar o arquivo de zona no Route 53. (Nem todos os provedores de serviço de DNS disponibilizam os arquivos de zona.) Quando você importa um arquivo de zona, o Route 53 reproduz automaticamente a configuração existente, criando os registros correspondentes em sua zona hospedada.

  Entre em contato com o suporte ao cliente do atual provedor de serviço de DNS para obter um arquivo de zona ou uma lista de registros. Para mais informações sobre o formato exigido do arquivo de zona, consulte Criar registros importando um arquivo de zona.
- Se a sua configuração DNS atual for mais complexa, e você estiver interessado nos recursos de roteamento do Route 53: analise a documentação a seguir para ver se deseja usar os recursos do

Route 53 que não estão disponíveis em outros provedores de serviço DNS. Se for o caso, você pode criar registros manualmente ou pode importar um arquivo de zona e, em seguida, criar ou atualizar registros posteriormente:

- Escolher entre registros de alias e não alias explica as vantagens de registros com alias do Route 53, que encaminham o tráfego para alguns recursos da AWS, como distribuições do CloudFront e buckets do Amazon S3, gratuitamente.
- A Escolher uma política de roteamento explica as opções de roteamento do Route 53, por exemplo, roteamento com base na localização de seus usuários, roteamento com base na latência entre seus usuários e seus recursos, roteamento com base na integridade de seus recursos e roteamento para recursos com base em ponderações especificadas por você.

> **Note**
>
> Você também pode importar um arquivo de zona e depois alterar sua configuração de aproveitar os registros de alias e as políticas de roteamento complexas.

Se não for possível obter um arquivo de zona ou se você quiser criar registros manualmente no Route 53, os registros que você vai migrar incluirão o seguinte:

- A (Address) records (Registros A (Endereço): associam um nome de domínio ou um nome de subdomínio ao endereço IPv4 (por exemplo, 192.0.2.3) do recurso correspondente
- AAAA (Address) records (Registros AAAA (Endereço): associam um nome de domínio ou um nome de subdomínio ao endereço IPv6 (por exemplo, 2001:0db8:85a3:0000:0000:abcd:0001:2345) do recurso correspondente
- Mail server (MX) records (Registros de servidor de e-mail (MX): encaminham tráfego para os servidores de e-mail
- CNAME records (Registros CNAME): reencaminham o tráfego de um nome de domínio (exemplo.net) para outro nome de domínio (exemplo.com)
- Records for other supported DNS record types (Registros de outros tipos de registros DNS compatíveis): para obter uma lista de tipos de registros compatíveis, consulte Tipos de registro de DNS com suporte.

Etapa 2: criar uma zona hospedada (domínios inativos)

Para informar ao Amazon Route 53 como você quer encaminhar o tráfego para seu domínio, crie uma zona hospedada com o mesmo nome que o seu domínio e, em seguida, crie registros nela.

> **Important**
>
> Você pode criar uma zona hospedada somente para um domínio que você tenha permissão para administrar. Normalmente, isso significa que você tem o domínio, mas também pode estar desenvolvendo uma aplicação para o proprietário dele.

Quando você cria uma zona hospedada, o Route 53 cria automaticamente um registro de servidor de nome (NS) e de início de autoridade (SOA) para a zona. O registro NS identifica os quatro servidores de nome que o Route 53 associou à sua zona hospedada. Para tornar o Route 53 o serviço de DNS do seu domínio, atualize o registro do domínio para usar esses quatro servidores de nome.

> **Important**
>
> Não crie registros adicionais de NS (servidor de nome) ou SOA (início de autoridade) e não exclua os registros de NS e SOA existentes.

Para criar uma zona hospedada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Se você for novo no Route 53, escolha Get started (Conceitos básicos).

   Se você já estiver usando o Route 53, escolha Hosted zones (Zonas hospedadas) no painel de navegação.
3. Escolha Create hosted zone (Criar zona hospedada).
4. No painel Create hosted zone (Criar zona hospedada), insira um nome de domínio e, se preferir, um comentário. Para obter mais informações sobre uma configuração, deixe o ponteiro do mouse sobre o rótulo para ver uma dica de ferramenta.

Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

5. Para Record type (Tipo de registro), aceite o valor padrão da Public hosted zone (Zona hospedada pública).
6. Escolha Create hosted zone (Criar zona hospedada).

Etapa 3: criar registros (domínios inativos)

Depois de criar uma zona hospedada, crie registros na zona hospedada que define onde você deseja redirecionar o tráfego para um domínio (exemplo.com) ou subdomínio (www.exemplo.com). Por exemplo, se você deseja encaminhar o tráfego para exemplo.com e www.exemplo.com para um servidor Web em uma instância do Amazon EC2, crie dois registros, um chamado exemplo.com e o outro chamado www.exemplo.com. Em cada registro, especifique o endereço IP para sua instância do EC2.

Você pode criar registros em uma série de formas:

Importar um arquivo de zona

Este é o método mais fácil se você tiver um arquivo de zona do seu serviço de DNS atual em Etapa 1: descobrir a configuração atual do DNS com o provedor de serviço de DNS atual (domínios inativos). O Amazon Route 53 não prevê quando deve criar registros de alias ou usar tipos de roteamento especiais, como ponderado ou failover. Como resultado, se você importar um arquivo de zona, o Route 53 cria registros de DNS padrão usando a política de roteamento simples.

Para obter mais informações, consulte Criar registros importando um arquivo de zona.

Criar registros individualmente no console

Se você não obteve o arquivo de zona e apenas deseja criar alguns registros com uma política de roteamento Simples para começar, você pode criar os registros no console do Route 53. Você pode criar registros com alias e sem alias.

Para mais informações, consulte os tópicos a seguir:

- Escolher uma política de roteamento
- Escolher entre registros de alias e não alias

- Criar registros usando o console do Amazon Route 53

Criar registros de forma programática

Você pode criar registros usando um dos SDKs, a AWS CLI ou o AWS Tools for Windows PowerShell da AWS. Para obter mais informações, consulte a Documentação do AWS.

Se você estiver usando uma linguagem de programação para a qual a AWS não fornece um SDK, você também pode usar a API do Route 53. Para obter mais informações, consulte Referência de API do Amazon Route 53.

Etapa 4: Atualizar o registro de domínio para usar servidores de nome do Amazon Route 53 (domínios inativos)

Após a criação dos registros para o domínio, você pode alterar o serviço de DNS do seu domínio para o Amazon Route 53. Execute o seguinte procedimento para atualizar as configurações com o registrador de domínio.

Para atualizar os servidores de nome para o domínio

1. No console do Route 53, obtenha os servidores de nome para sua zona hospedada do Route 53:

   a. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   b. No painel de navegação, escolha Zonas hospedadas.

   c. Na página Hosted zones (Zonas hospedadas), escolha o botão de opção (não o nome) da zona hospedada, depois escolha View details (Exibir detalhes).

   d. Na página de detalhes da zona hospedada, escolha Hosted zone details (Detalhes da zona hospedada).

   e. Anote os quatro servidores listados para Name servers (Servidores de nome).

2. Use o método fornecido pelo registrador para o domínio a fim de alterar os servidores de nome para o domínio usar os quatro servidores de nome do Route 53 que você obteve na etapa 2 deste procedimento.

   Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

Configurar o roteamento de DNS para um novo domínio

Ao registrar um domínio com o Route 53, nós automaticamente tornamos o Route 53 o serviço DNS do domínio. O Route 53 cria uma zona hospedada com o mesmo nome do domínio, atribui quatro servidores de nomes à zona hospedada e atualiza o domínio para usar esses servidores de nomes.

Para especificar como você quer que o Route 53 encaminhe o tráfego da Internet para o domínio, crie registros na zona hospedada. Por exemplo, se você quiser encaminhar solicitações de example.com para um servidor da Web que é executado em uma instância do Amazon EC2, crie um registro na zona hospedada de example.com e especifique o endereço de IP elástico para a instância do EC2. Para obter mais informações, consulte os tópicos a seguir.

- Para obter informações sobre como criar registros na sua zona hospedada, consulte Trabalhar com registros.
- Para obter informações sobre como rotear o tráfego para AWS recursos selecionados, consulteEncaminhando o tráfego da Internet para seus recursos AWS.
- Para informações sobre como o DNS funciona, consulte Como o tráfego da Internet é roteado para seu site ou o aplicativo web.

Rotear tráfego para seus recursos

Quando os usuários solicitam seu site ou aplicação Web, por exemplo, inserindo o nome de seu domínio em um navegador da Web, o Amazon Route 53 ajuda a encaminhar os usuários para seus recursos, como um bucket do Amazon S3 ou um servidor da Web em seu datacenter. Se você quiser configurar o Route 53 para encaminhar o tráfego para os seus recursos, faça o seguinte:

1. Crie uma zona hospedada. Você pode criar uma zona hospedada pública ou privada:

   Zona hospedada pública

   Crie uma zona hospedada pública se você quiser direcionar o tráfego da Internet para os seus recursos, por exemplo, para que seus clientes possam visualizar o site da empresa que você está hospedando nas instâncias do EC2. Para obter mais informações, consulte Trabalhar com zonas hospedadas públicas.

Zonas hospedadas privadas

Crie uma zona hospedada privada se você quiser encaminhar o tráfego dentro de uma Amazon VPC. Para obter mais informações, consulte Trabalhar com zonas hospedadas privadas.

2. Crie registros na zona hospedada. Os registros definem onde você quer rotear o tráfego para cada nome de domínio ou de subdomínio. Por exemplo, para rotear o tráfego de www.example.com para um servidor da web no seu datacenter, você pode criar um registro www.example.com na zona hospedada example.com.

   Para obter mais informações, consulte os tópicos a seguir:

   - Trabalhar com registros
   - Rotear tráfego para subdomínios
   - Encaminhando o tráfego da Internet para seus recursos AWS

Rotear tráfego para subdomínios

Quando quiser rotear o tráfego para recursos de um subdomínio, como acme.example.com ou zenith.example.com, você terá duas opções:

Criar registros na zona hospedada para o domínio

Normalmente, para rotear o tráfego de um subdomínio, você cria um registro na zona hospedada com o mesmo nome do domínio. Por exemplo, para rotear o tráfego da Internet de acme.example.com para um servidor da web no seu datacenter, crie um registro denominado acme.example.com na zona hospedada example.com. Para obter mais informações, consulte o tópico Trabalhar com registros e seus subtópicos.

Criar uma zona hospedada para o subdomínio e registros na nova zona hospedada

Você também pode criar uma zona hospedada para o subdomínio. O uso de uma zona hospedada separada para rotear o tráfego da Internet para um subdomínio às vezes é chamado de "delegar a responsabilidade por um subdomínio a uma zona hospedada" ou "delegar um subdomínio a outros servidores de nome" ou alguma combinação semelhante de termos. Esta é uma visão geral de como isso funciona:

1. Crie uma zona hospedada que tenha o mesmo nome que o subdomínio para o qual você deseja rotear o tráfego, como acme.example.com.

2. Depois, crie registros na nova zona hospedada que definam como você quer rotear o tráfego para o subdomínio (acme.example.com) e seus subdomínios, como backend.acme.example.com.
3. Você obterá os servidores de nomes que o Route 53 atribuiu à nova zona hospedada quando você a criou.
4. Crie um novo registo NS na zona hospedada para o domínio (example.com) e especifique os quatro servidores de nomes obtidos na etapa 3.

Quando você usa uma zona hospedada separada para rotear tráfego para um subdomínio, pode usar as permissões do IAM para restringir o acesso à zona hospedada dele. Se você tiver vários subdomínios gerenciados por grupos diferentes, a criação de uma zona hospedada para cada subdomínio pode reduzir significativamente o número de pessoas que precisam ter acesso a registros na zona hospedada para o domínio.

O uso de uma zona hospedada separada para um subdomínio também permite que você use diferentes serviços de DNS para o domínio e o subdomínio. Para obter mais informações, consulte Como usar o Amazon Route 53 como o serviço DNS dos subdomínios sem migrar o domínio pai.

Há um pequeno impacto na performance com essa configuração na primeira consulta DNS de cada resolvedor de DNS. O resolvedor precisa obter informações da zona hospedada para o domínio raiz e, em seguida, informações da zona hospedada para o subdomínio. Após a primeira consulta DNS em um subdomínio, o resolvedor armazena em cache as informações e não precisa obtê-las novamente até que o TTL expire e outro cliente solicite o subdomínio desse resolvedor. Para mais informações, consulte TTL (segundos) na seção Valores que você especifica ao criar ou editar registros do Amazon Route 53.

Tópicos

- Criar outra zona hospedada para rotear o tráfego de um subdomínio
- Rotear tráfego para níveis adicionais de subdomínios

Criar outra zona hospedada para rotear o tráfego de um subdomínio

Uma maneira de rotear o tráfego para um subdomínio é criar uma zona hospedada para o subdomínio e criar registros para o subdomínio na nova zona hospedada. (A opção mais comum é criar registros para o subdomínio na zona hospedada do domínio.)

> **Note**
>
> Embora descrevamos aqui o processo para criar e delegar a uma zona hospedada de subdomínio no Route 53, você também pode criar uma zona DNS em outros servidores de nomes e, de forma semelhante, criar registros de servidor de nomes (NS) que delegam responsabilidade a esses servidores de nomes.

Aqui está uma visão geral do processo:

1. Crie uma zona hospedada do para o subdomínio. Para obter mais informações, consulte Criar uma nova zona hospedada para um subdomínio.
2. Adicione registros à zona hospedada para o subdomínio. Se a zona hospedada do domínio contiver algum registro que pertence à zona hospedada do subdomínio, duplique esses registros na zona hospedada do subdomínio. Para obter mais informações, consulte Criar registros na zona hospedada do subdomínio
3. Crie um registro NS para o subdomínio na zona hospedada do domínio, que delega a responsabilidade pelo subdomínio aos servidores de nome na nova zona hospedada. Se a zona hospedada do domínio contiver algum registro que pertence à zona hospedada do subdomínio, exclua os registros da zona hospedada do domínio. (Você criou cópias na zona hospedada do subdomínio na etapa 2.) Para obter mais informações, consulte Atualizar a zona hospedada do domínio.

Criar uma nova zona hospedada para um subdomínio

Para criar uma zona hospedada para um subdomínio usando o console do Route 53, execute o seguinte procedimento.

Para criar uma zona hospedada para um subdomínio (console)

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Se você for novo no Route 53, escolha Get started (Conceitos básicos).

   Se você já estiver usando o Route 53, escolha Hosted zones (Zonas hospedadas) no painel de navegação.
3. Escolha Create hosted zone (Criar zona hospedada).

4. No painel direito, insira o nome do subdomínio, como acme.example.com. Se preferir, você também pode inserir um comentário.

   Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.
5. Para Type (Tipo), aceite o valor padrão da Public hosted zone (Zona pública hospedada).
6. Na parte inferior do painel à direita, escolha Create hosted zone (Criar zona hospedada).

Criar registros na zona hospedada do subdomínio

Para definir como você quer que o Route 53 encaminhe o tráfego para o subdomínio (acme.example.com) e seus subdomínios (backend.acme.example.com), crie registros na zona hospedada do subdomínio.

Observe o seguinte sobre como criar registros na zona hospedada do subdomínio:

- Não crie registros de NS (servidor de nome) ou SOA (início de autoridade) adicionais na zona hospedada do subdomínio nem exclua os registros de NS e SOA existentes.
- Crie todos os registros do subdomínio na zona hospedada dele. Por exemplo, se você tiver zonas hospedadas dos domínios example.com e acme.example.com, crie todos os registros do subdomínio acme.example.com na zona hospedada de acme.example.com. Isso inclui registros como backend.acme.example.com e beta.backend.acme.example.com.
- Se a zona hospedada do domínio (example.com) já contiver registros que pertencem à zona hospedada do subdomínio (acme.example.com), duplique esses registros na zona hospedada do subdomínio. Na última etapa do processo, exclua os registros duplicados da zona hospedada do domínio mais tarde.

> **Important**
>
> Se você tiver alguns registros do subdomínio nas zonas hospedadas do domínio e do subdomínio, o comportamento do DNS será inconsistente. O comportamento dependerá de quais servidores de nome um resolvedor de DNS possui em cache, dos servidores de nome da zona hospedada do domínio (example.com) ou dos servidores de nome da zona hospedada do subdomínio (acme.example.com). Em alguns casos, o Route 53 retornará NXDOMAIN (domínio inexistente) quando o registro existir, mas não na zona hospedada à qual os resolvedores de DNS estão enviando a consulta.

Para obter mais informações, consulte Trabalhar com registros.

Atualizar a zona hospedada do domínio

Quando você cria uma zona hospedada, o Route 53 atribui automaticamente quatro servidores de nome à zona. O registro NS de uma zona hospedada identifica os servidores de nome que respondem às consultas DNS do domínio ou do subdomínio. Para começar a usar os registros na zona hospedada do subdomínio e rotear o tráfego da Internet, crie um novo registro NS na zona hospedada do domínio (example.com) e atribua a ele o nome do subdomínio (acme.example.com). Para o valor do registro NS, especifique os nomes dos servidores de nome da zona hospedada do subdomínio.

Veja o que acontece quando o Route 53 recebe uma consulta DNS de um resolvedor DNS para o subdomínio acme.example.com ou um dos seus subdomínios:

1. O Route 53 procura o domínio (example.com) na zona hospedada e localiza o registro NS para o subdomínio (acme.example.com).
2. O Route 53 obtém os servidores de nome do registro NS acme.example.com na zona hospedada do domínio, example.com, e retorna esses servidores de nome para o resolvedor de DNS.
3. O resolvedor de reenvia a consulta de acme.example.com aos servidores de nome da zona hospedada acme.example.com.
4. O Route 53 responde à consulta usando um registro na zona hospedada acme.example.com.

Para configurar o Route 53 para encaminhar o tráfego para o subdomínio usando a zona hospedada do subdomínio e excluir todos os registros duplicados da zona hospedada do domínio, realize o procedimento a seguir:

Para configurar o Route 53 para usar a zona hospedada do subdomínio (console)

1. No console do Route 53, veja os servidores de nome para a zona hospedada do subdomínio:
    a. No painel de navegação, escolha Zonas hospedadas.
    b. Na página Hosted zones (Zonas hospedadas), escolha o nome para a zona hospedada do subdomínio.
    c. No painel direito, copie os nomes dos quatro servidores listados para Name servers (Servidores de nome) na seção Hosted zones details (Detalhes das zonas hospedadas).
2. Escolha o nome da zona hospedada para o domínio (example.com), não para o subdomínio.

3. Escolha Create record (Criar registro).
4. Escolha Simple routing (Roteamento simples) e Next (Próximo).
5. Escolha Define simple record (Definir registro simples).
6. Especifique os seguintes valores:

   Name (Nome)

   Insira o nome do subdomínio.

   Valor/Encaminhar tráfego para

   Escolha endereço IP ou outro valor dependendo do tipo de registro e cole os nomes dos servidores de nome que você copiou na etapa 1.

   Tipo de registro

   Escolha NS – Name servers for a hosted zone (NS: servidores de nome para uma zona hospedada).

   TTL (segundos)

   Altere para um valor mais comum para um registro NS, como 172.800 segundos.
7. Selecione Define simple record (Definir registro simples) e escolha Create records (Criar registros).
8. Se a zona hospedada do domínio contiver algum registro que você recriou na zona hospedada do subdomínio, exclua esses registros da zona hospedada do domínio. Para obter mais informações, consulte Excluir registros.

   Quando terminar, todos os registros do subdomínio deverão estar na zona hospedada do subdomínio.

Rotear tráfego para níveis adicionais de subdomínios

Direcione o tráfego para o subdomínio de um subdomínio, como backend.acme.example.com, da mesma forma que você direciona o tráfego para um subdomínio, como acme.example.com. Crie registros na zona hospedada do domínio ou uma zona hospedada para o subdomínio de nível inferior e, em seguida, crie registros nessa nova zona hospedada.

Se você optar por criar uma zona hospedada para o subdomínio de nível inferior, crie o registro de NS para o subdomínio de nível inferior na zona hospedada para o subdomínio que está um nível

mais próximo do nome de domínio. Isso ajuda a garantir que o tráfego seja roteado corretamente para os recursos. Por exemplo, suponhamos que você queira rotear o tráfego para os seguintes subdomínios:

- subdomain1.example.com
- subdomain2.subdomain1.example.com

Se você quiser usar outra zona hospedada para rotear o tráfego para subdomínio2.subdomínio1.example.com, faça o seguinte:

1. Crie uma zona hospedada chamada subdomain2.subdomain1.example.com.
2. Crie registros na zona hospedada subdomain2.subdomain1.example.com. Para obter mais informações, consulte Criar registros na zona hospedada do subdomínio.
3. Copie os nomes dos servidores de nome para a zona hospedada subdomain2.subdomain1.example.com.
4. Na zona hospedada subdomain1.example.com, crie um registro NS denominado subdomain2.subdomain1.example.com e cole os nomes dos servidores de nome da zona hospedada subdomain2.subdomain1.example.com.

   Além disso, exclua todos os registros duplicados de subdomain1.example.com. Para obter mais informações, consulte Atualizar a zona hospedada do domínio.

   Depois de criar este registro NS, o Route 53 começa a usar a zona hospedada subdomain2.subdomain1.example.com para encaminhar o tráfego para o subdomínio subdomain2.subdomain1.example.com.

Trabalhar com zonas hospedadas

Uma zona hospedada é um contêiner para registros, e os registros contêm informações sobre como você quer rotear o tráfego para um domínio específico, como example.com e seus subdomínios (apex.example.com, acme.example.com). Uma zona hospedada e o domínio correspondente têm o mesmo nome. Há dois tipos de zonas hospedadas:

- Zonas hospedadas públicas contém registros que especificam a forma como você quer rotear o tráfego na Internet. Para ter mais informações, consulte Trabalhar com zonas hospedadas públicas.

- Zonas hospedadas privadas contém registros que especificam a forma como você quer rotear o tráfego na Amazon VPC. Para ter mais informações, consulte Trabalhar com zonas hospedadas privadas.

Trabalhar com zonas hospedadas públicas

Uma zona hospedada pública é um contêiner que armazena informações sobre como você deseja rotear o tráfego de um domínio específico (como example.com) e subdomínios (como acme.example.com, zenith.example.com) na Internet. Você recebe uma zona hospedada pública de duas maneiras:

- Quando você registra um domínio com o Route 53, nós criamos automaticamente uma zona hospedada para você.
- Ao transferir o serviço DNS de um domínio existente para o Route 53, comece criando uma zona hospedada para o domínio. Para obter mais informações, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Em ambos os casos, você cria registros na zona hospedada para especificar a maneira como deseja rotear o tráfego para o domínio e os subdomínios. Por exemplo, você pode criar um registro para encaminhar o tráfego de www.example.com para uma distribuição do CloudFront ou para um servidor da Web no seu datacenter. Para obter mais informações sobre registros de , consulte Trabalhar com registros.

Este tópico explica como usar o console do Amazon Route 53 para criar, listar e excluir zonas hospedadas públicas.

> **Note**
>
> Você também pode usar uma zona hospedada privada do Route 53 para encaminhar o tráfego em uma ou mais VPCs criadas com o serviço da Amazon VPC. Para obter mais informações, consulte Trabalhar com zonas hospedadas privadas.

Tópicos

- Listar zonas hospedadas públicas
- Visualizar métricas de consulta de DNS para uma zona hospedada pública
- Excluir uma zona hospedada pública
- Verificar respostas do Route 53 ao DNS
- Configurar servidores de nome de rótulo branco
- Registros de NS e SOA que o Amazon Route 53 cria para uma zona hospedada pública

Considerações ao trabalhar com zonas hospedadas públicas

Veja as seguintes considerações ao trabalhar com zonas hospedadas públicas:

Registros de NS e SOA

Quando você cria uma zona hospedada, o Amazon Route 53 cria automaticamente um registro de servidor de nome (NS) e de início de autoridade (SOA) para a zona. O registro de NS identifica os quatro servidores de nome que você fornece ao seu registrador ou ao serviço DNS, de maneira que as consultas de DNS sejam encaminhadas aos servidores de nome do Route 53. Para obter mais informações sobre registros de NS e SOA, consulte Registros de NS e SOA que o Amazon Route 53 cria para uma zona hospedada pública.

Várias zonas hospedadas que possuem o mesmo nome

Você pode criar mais de uma zona hospedada com o mesmo nome e adicionar diferentes registros a cada zona hospedada. O Route 53 atribui quatro servidores de nome a cada zona hospedada, e os servidores de nome são diferentes para cada uma delas. Ao atualizar os registros de servidor de nome do registrador, tome cuidado para usar os servidores de nome do Route 53 para a zona hospedada correta, isto é, aquela que contém os registros que você quer que o Route 53 use ao responder às consultas do seu domínio. O Route 53 nunca retorna valores para registros em outras zonas hospedadas que têm o mesmo nome.

Conjuntos de delegações reutilizáveis

Por padrão, o Route 53 atribui um conjunto exclusivo de quatro servidores de nome (conhecido coletivamente como um conjunto de delegações) a cada zona hospedada que você cria.
Se quiser criar um grande número de zonas hospedadas, você poderá criar um conjunto de delegações reutilizáveis de maneira programática. (Conjuntos de delegação reutilizáveis não estão disponíveis no console do Route 53.) Em seguida, você pode criar zonas hospedadas de forma programada e atribuir o mesmo conjunto de delegações reutilizáveis, os mesmos quatro servidores de nome, a cada zona hospedada.

Os conjuntos de delegações reutilizáveis simplificam a migração do serviço DNS para o Route 53 porque você pode instruir o registrador do nome do domínio a usar os mesmos quatro servidores de nome para todos os domínios para os quais você quer usar o Route 53 como o serviço DNS. Para mais informações, consulte CreateReusableDelegationSet na Referência da API do Amazon Route 53.

Criar uma zona hospedada pública

Uma zona hospedada pública é um contêiner que armazena informações sobre como você deseja rotear o tráfego de um domínio específico (como example.com) e subdomínios (como acme.example.com, zenith.example.com) na Internet. Depois de criar uma zona hospedada, você cria registros que especificam a maneira como deseja rotear o tráfego para o domínio e os subdomínios.

> **Important**
>
> Você pode criar uma zona hospedada somente para um domínio que você tenha permissão para administrar. Normalmente, isso significa que você tem o domínio, mas também pode estar desenvolvendo uma aplicação para o proprietário dele.

Para criar uma zona hospedada pública usando o console do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Se você for novo no Route 53, escolha Get started (Conceitos básicos) em DNS Management (Gerenciamento de DNS).

   Se você já estiver usando o Route 53, escolha Hosted zones (Zonas hospedadas) no painel de navegação.
3. Escolha Create hosted zone (Criar zona hospedada).
4. No painel Create Hosted Zone (Criar zona hospedada), insira o nome do domínio para o qual você deseja rotear o tráfego. Se preferir, você também pode inserir um comentário.

   Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

5. Para Type, aceite o valor padrão da Public Hosted Zone.
6. Escolha Create (Criar).
7. Crie registros que especificam a maneira como você deseja rotear o tráfego para o domínio e os subdomínios. Para obter mais informações, consulte Trabalhar com registros.
8. Para usar registros na nova zona hospedada para rotear o tráfego de seu domínio, consulte o tópico aplicável:

   - Se estiver tornando o Route 53 o serviço DNS de um domínio registrado em outro registrador de domínios, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.
   - Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

Obter os servidores de nome de uma zona hospedada pública

Obtenha os servidores de nome para uma zona hospedada pública se desejar alterar o serviço de DNS para o registro de domínio. Para obter informações sobre como alterar o serviço de DNS, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

> **Note**
>
> Alguns registradores só permitem que você especifique servidores de nome usando endereços IP; eles não permitem que você especifique nomes de domínio totalmente qualificados. Se o seu registrador requer o uso de endereços IP, você pode obter os endereços IP para os seus servidores de nome usando o utilitário dig (para Mac, Unix ou Linux) ou o utilitário nslookup (para Windows). Raramente alteramos os endereços IP de servidores de nome; se precisarmos alterar endereços IP, você será notificado com antecedência.

Para obter os servidores de nome de uma zona hospedada usando o console do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, clique em Hosted zones (Zonas hospedadas).
3. Na página Hosted zones (Zonas hospedadas), escolha o botão de opção (não o nome) da zona hospedada, depois escolha View details (Exibir detalhes).

4. Na página de detalhes da zona hospedada, escolha Hosted zone details (Detalhes da zona hospedada).
5. Anote os quatro servidores listados para Name servers (Servidores de nome).

Listar zonas hospedadas públicas

Você pode usar o console do Amazon Route 53 para listar todas as zonas hospedadas criadas com a conta da AWS atual. Para obter informações sobre como listar zonas hospedadas usando a API do Route 53, consulteListHostedZones na Referência da API do Amazon Route 53.

Para listar as zonas hospedadas públicas associadas a uma conta da AWS usando o console do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas. A página exibe uma lista de zonas hospedadas que estão associadas à conta da AWS na qual você está conectado.
3. Para filtrar zonas hospedadas, use a barra de pesquisa localizada na parte superior da tabela.

   O comportamento de pesquisa variará quando a zona hospedada tiver até 2 mil registros e mais de 2 mil registros:

   Até 2 mil zonas hospedadas

   - Para exibir os registros que têm valores específicos, clique na barra de pesquisa, escolha uma propriedade na lista suspensa e insira um valor. Também é possível inserir um valor diretamente na barra de pesquisa e pressionar Enter. Por exemplo, para exibir as zonas hospedadas que têm um nome começando com **abc**, insira esse valor na barra de pesquisa e pressione Enter.
   - Para exibir somente as zonas hospedadas que têm o mesmo tipo de zona hospedada, selecione o tipo na lista suspensa e insira o tipo.

   Mais de 2 mil zonas hospedadas

   - Você pode pesquisar propriedades com base no nome de domínio exato, todas as propriedades e tipo.
   - Pesquise usando o nome de domínio exato para obter resultados de pesquisa mais rápidos.

Visualizar métricas de consulta de DNS para uma zona hospedada pública

Você pode visualizar o número total de consultas de DNS que o Route 53 está respondendo para uma zona hospedada pública especificada ou uma combinação de zonas hospedadas públicas. As métricas são exibidas no CloudWatch, o que permite visualizar um gráfico, escolher o período que você quer visualizar e personalizar as métricas de várias outras maneiras. Você também pode criar alarmes e configurar notificações, para que possa ser notificado quando o número de consultas de DNS em um período especificado ficar acima ou abaixo de um nível especificado.

> **Note**
>
> O Route 53 envia automaticamente o número de consultas de DNS ao CloudWatch para todas as zonas hospedadas públicas, portanto, você não precisa configurar nada para conseguir visualizar as métricas de consulta. As métricas de consulta de DNS não são cobradas.

Que consultas de DNS são contabilizadas?

As métricas incluem apenas as consultas que os resolvedores de DNS encaminham ao Route 53. Se o resolvedor de DNS já tiver armazenado em cache a resposta a uma consulta (como o endereço IP de um balanceador de carga para example.com), o resolvedor continuará retornando a resposta armazenada em cache sem encaminhar a consulta para o Route 53 até que o TTL do registro correspondente expire.

Dependendo da quantidade de consultas de DNS enviadas para um nome de domínio (example.com) ou nome de subdomínio (www.example.com), de quais resolvedores seus usuários estão usando e do TTL do registro, as métricas de consulta de DNS podem conter informações apenas sobre uma das milhares de consultas que são enviadas aos resolvedores de DNS. Para mais informações sobre como o DNS funciona, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

Quando as métricas de consulta para uma zona hospedada começam a ser exibidas no CloudWatch?

Depois de criar uma zona hospedada, poderá levar várias horas para que a zona hospedada seja exibida no CloudWatch. Além disso, você deverá enviar uma consulta de DNS para um registro na zona hospedada para que haja dados a serem exibidos.

As métricas estão disponíveis somente no Leste dos EUA (Norte da Virgínia)

Para obter métricas no console, você deve escolher Leste dos EUA (Norte da Virgínia) para a região. Para obter métricas usando a CLI da AWS, você deve deixar a região da AWS não especificada ou especificar `us-east-1` como a região. As métricas do Route 53 não estarão disponíveis se você escolher qualquer outra região.

Métrica e dimensão do CloudWatch para consultas de DNS

Para obter informações sobre a métrica e a dimensão do CloudWatch para consultas de DNS, consulte Monitoramento de zonas hospedadas usando a Amazon CloudWatch. Para obter mais informações sobre métricas e alarmes do CloudWatch, consulte Como usar as métricas do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

Obter dados mais detalhados sobre consultas de DNS

Para obter informações mais detalhadas sobre cada consulta de DNS à qual o Route 53 responde, incluindo os seguintes valores, você pode configurar o log de consultas:

- O domínio ou o subdomínio que foi solicitado
- Data e hora da solicitação
- Tipo de registro DNS (como A ou AAAA)
- O ponto de presença do Route 53 que respondeu à consulta DNS
- O código de resposta DNS, como `NoError` ou `ServFail`

Para obter mais informações, consulte Log de consultas de DNS pública.

Como obter métricas de consulta de DNS

Logo após a criação de uma zona hospedada, o Amazon Route 53 começa a enviar métricas e dimensões, uma vez por minuto para o CloudWatch. Você pode usar os procedimentos a seguir para visualizar as métricas no console do CloudWatch ou visualizá-las usando a AWS Command Line Interface (AWS CLI).

Tópicos

- Visualizar métricas de consulta de DNS para uma zona hospedada pública no console do CloudWatch
- Obter métricas de consulta de DNS usando a AWS CLI

Visualizar métricas de consulta de DNS para uma zona hospedada pública no console do CloudWatch

Para visualizar métricas de consulta de DNS para zonas hospedadas públicas no console do CloudWatch, execute o procedimento a seguir.

Para visualizar métricas de consulta de DNS para uma zona hospedada pública no console do CloudWatch

1. Faça login no AWS Management Console e abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Metrics (Métricas).
3. Na lista de regiões da AWS, no canto superior direito do console, escolha US East (N. Virginia) (Leste dos EUA [Norte da Virgínia]). As métricas do Route 53 não estarão disponíveis se você escolher qualquer outra região da AWS.
4. Na guia Todas as métricas, escolha Route 53.
5. Escolha Hosted Zone Metrics (Métricas de zona hospedada).
6. Marque a caixa de seleção de uma ou mais zonas hospedadas que tenham o nome de métrica DNSQueries.
7. Na guia Graphed metrics (Métricas em gráfico), altere os valores aplicáveis para visualizar as métricas no formato desejado.

   Em Statistic (Estatística), escolha Sum (Soma) ou SampleCount; essas estatísticas exibem o mesmo valor.

Obter métricas de consulta de DNS usando a AWS CLI

Para obter métricas de consulta de DNS usando a AWS CLI, use o comando get-metric-data. Observe o seguinte:

- Você especifica a maioria dos valores para o comando em um arquivo JSON separado. Para obter mais informações, consulte get-metric-data.
- O comando retorna um valor para cada intervalo especificado para `Period` no arquivo JSON. O `Period` está em segundos, portanto, se você especificar um período de cinco minutos e especificar `60` para `Period`, receberá cinco valores. Se você especificar um período de cinco minutos e especificar `300` para `Period`, receberá um valor.
- No arquivo JSON, você pode especificar qualquer valor para `Id`.

- Deixe a região da AWS não especificada ou especifique `us-east-1` como a região. As métricas do Route 53 não estarão disponíveis se você escolher qualquer outra região. Para obter mais informações, consulte Configuração da CLI da AWS no Manual do usuário da AWS Command Line Interface.

Este é o comando da AWS CLI que você usa para obter métricas de consulta de DNS para o período de cinco minutos entre as 4:01 e as 4:07 em 1º de maio de 2019. O parâmetro `metric-data-queries` faz referência ao arquivo JSON de exemplo que segue o 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
```

Aqui está o arquivo JSON de exemplo:

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

Veja a saída desse comando. Observe o seguinte:

- Os horários de início e de término no comando abrangem um período de sete minutos, `2019-05-01T04:01:00Z` a `2019-05-01T04:07:00Z`.

- Há apenas seis valores de retorno. Não há nenhum valor para `2019-05-01T04:05:00Z` porque não houve consultas de DNS durante esse minuto.
- O valor de `Period` especificado no arquivo JSON é `60` (segundos), portanto, os valores são relatados em intervalos de um 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"
            ]
        }
    ]
}
```

Excluir uma zona hospedada pública

Esta seção explica como excluir uma zona hospedada pública usando o console do Amazon Route 53.

Você só pode excluir uma zona hospedada se não houver outros registros que não sejam os registros padrão de SOA e de NS. Se a sua zona hospedada contiver outros registros, você precisará excluí-los antes de excluir a zona hospedada. Isso evita que você exclua acidentalmente uma zona hospedada que ainda contém registros.

Tópicos

Impedir que o tráfego seja roteado para seu domínio

Para manter o registro do domínio, mas interromper o roteamento do tráfego da Internet para seu site ou aplicativo web, recomendamos excluir os registros na zona hospedada em vez de excluir a zona hospedada.

> **Important**
>
> Se você excluir uma zona hospedada, não será possível pode cancelar a exclusão. É necessário criar outra zona hospedada e atualizar os servidores de nome para o registro do domínio, o que pode levar até 48 horas para entrar em vigor. Além disso, se você excluir uma zona hospedada, alguém poderá sequestrar o domínio e rotear o tráfego para seus próprios recursos usando seu nome de domínio.
>
> Se você delegar a responsabilidade de um subdomínio para uma zona hospedada e quiser excluir a zona hospedada filha, será necessário atualizar a zona hospedada pai excluindo o registro NS que tenha o mesmo nome que a zona hospedada filha. Por exemplo, se quiser excluir a zona hospedada acme.example.com, será necessário excluir também o registro NS acme.example.com na zona hospedada example.com. Recomendamos excluir o registro NS primeiro e aguardar a duração do TTL no registro NS antes de excluir a zona hospedada filha. Isso garante que ninguém conseguirá sequestrar a zona hospedada filha enquanto os resolvedores DNS tiverem os servidores de nomes para a zona hospedada filha em cache.

Se quiser evitar a cobrança mensal da zona hospedada, você poderá transferir o serviço de DNS do domínio para um serviço de DNS gratuito. Ao transferir o serviço de DNS, será necessário atualizar os servidores de nome do registro de domínio. Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio para obter informações sobre como substituir servidores de nome do Route 53 por servidores de nome do novo serviço DNS. Se o domínio estiver registrado com outro registrador, use o método fornecido pelo registrador para atualizar os servidores de nome do registro de domínio. Para mais informações, faça uma pesquisa na Internet sobre "serviço DNS gratuito".

Excluir zonas hospedadas públicas que foram criadas por outro serviço

Se uma zona hospedada foi criada por outro serviço, você não pode excluí-la usando o console do Route 53. Em vez disso, você precisa usar o processo aplicável para outros serviços:

- AWS Cloud Map: para excluir uma zona hospedada que o AWS Cloud Map criou quando você criou um namespace de DNS público, exclua o namespace. O AWS Cloud Map exclui a zona hospedada automaticamente. Para obter mais informações, consulte Deleting namespaces (Excluir namespaces) no AWS Cloud MapGuia do desenvolvedor.
- Descoberta de serviço do Amazon Elastic Container Service (Amazon ECS): para excluir uma zona hospedada pública que o Amazon ECS criou quando você criou um serviço usando a descoberta de serviço, exclua os serviços do Amazon ECS que estão usando o namespace e exclua o namespace. Para obter mais informações, consulte Como excluir um serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

Como usar o console do Route 53 para excluir uma zona hospedada pública

Para usar o console do Route 53 para excluir uma zona hospedada pública, execute o procedimento a seguir.

Para excluir uma zona hospedada pública usando o console do Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e escolha o link destacado da zona hospedada que deseja excluir.
3. Verifique se a zona hospedada que você deseja excluir contém apenas um registro NS e SOA. Se houver registros adicionais, exclua-os. Você também precisará desabilitar a assinatura de DNSSEC:

    - Na página de detalhes da zona hospedada, na lista Records (Registros), se a lista de registros incluir quaisquer registros para os quais o valor da coluna Type (Tipo) for diferente de NS ou SOA, escolha a linha e depois Delete (Excluir).

      Para selecionar vários registros consecutivos, escolha a primeira linha, mantenha a tecla Shift pressionada e selecione a última linha. Para selecionar vários registros não consecutivos, escolha a primeira linha, mantenha a tecla Ctrl pressionada e selecione as demais linhas.

> **Note**
>
> Se você criou registros de NS para subdomínios na zona hospedada, exclua esses registros também.

4. Volte para a página Hosted zones (Zonas hospedadas) e escolha a linha da zona hospedada que deseja excluir.
5. Escolha Delete (Excluir).
6. Digite a chave de confirmação e escolha Delete (Excluir).
7. Se pretender tornar o domínio indisponível na Internet, recomendamos que você transfira o serviço DNS para um serviço DNS gratuito e, em seguida, elimine a zona hospedada do Route 53. Isso impede que futuras consultas DNS sejam incorretamente encaminhadas.

   Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio para obter informações sobre como substituir servidores de nome do Route 53 por servidores de nome do novo serviço DNS. Se o domínio estiver registrado com outro registrador, use o método fornecido pelo registrador para alterar os servidores de nome do domínio.

   > **Note**
   >
   > Se você estiver excluindo uma zona hospedada de um subdomínio (acme.example.com), não será necessário alterar os servidores de nome do domínio (example.com).

Verificar respostas do Route 53 ao DNS

Se criou um zona hospedada do Amazon Route 53 para seu domínio, você poderá usar a ferramenta de verificação do DNS no console para ver como o Route 53 responderá às consultas DNS se você configurar seu domínio para usar o Route 53 como seu serviço DNS. Para os registros de latência, geolocalização e geoproximidade, também é possível simular consultas de determinado resolvedor de DNS e/ou endereço IP do cliente para descobrir a resposta que o Route 53 retornaria.

> **Important**
>
> A ferramenta não envia consultas ao Domain Name System (DNS). Ela só responde com base nas configurações nos registros na zona hospedada. A ferramenta retorna as mesmas informações independentemente de a zona hospedada estar sendo usada no momento para rotear o tráfego para o domínio.

A ferramenta de verificação de DNS funciona apenas para zonas hospedadas públicas.

> **Note**
>
> A ferramenta de verificação de DNS retorna informações semelhantes às que você esperaria da seção de resposta do comando `dig`. Portanto, se você solicitar os servidores de nomes de um subdomínio que apontam para os servidores de nomes superiores, eles não serão retornados.

Tópicos

Como usar a ferramenta de verificação para ver como o Amazon Route 53 responde às consultas de DNS

Você pode usar a ferramenta para ver a resposta do Amazon Route 53 a uma consulta de DNS para um registro.

Para usar a ferramenta de verificação para ver como o Route 53 responde às consultas de DNS

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Zonas hospedadas, escolha o nome de uma zona hospedada. O console exibe a lista de registros para essa zona hospedada.

4. Para ir diretamente para a página Check response from Route 53 (Verificar resposta do Route 53), escolha Test record (Testar registro).
5. Especifique os seguintes valores:
   - O nome do registro, excluindo o nome da zona hospedada. Por exemplo, para verificar www.example.com, insira www. Para verificar example.com, deixe o campo Record name (Nome do registro) em branco.
   - O tipo de registro que você deseja verificar, como A ou CNAME.
6. Escolha Obter resposta.
7. A seção Resposta retornada pelo Route 53 inclui os seguintes valores:

   Código de resposta do DNS

   Um código que indica se a consulta foi válida ou não. O código de resposta mais comum é NOERROR e indica que a consulta é válida. Se a resposta não for válida, o Route 53 retornará um código de resposta que explicará o motivo. Para obter uma lista dos códigos de resposta possíveis, consulte DNS RCODES no site da IANA.

   Protocolo

   O protocolo que o Amazon Route 53 usou para responder a consulta. O protocolo pode ser UDP ou TCP.

   Resposta retornada pelo Route 53

   O valor que o Route 53 retornaria para uma aplicação Web. O valor é um dos seguintes:
   - Para registros que não sejam de alias, a resposta contém um ou mais valores no registro.
   - Para vários registros que têm o mesmo nome e tipo, que inclui conjuntos ponderados, de latência, localização geográfica e failover, a resposta contém o valor do registro apropriado, de acordo com a solicitação.
   - Para registros de alias que fazem referência a outros recursos da AWS diferentes do registro, a resposta contém um endereço IP ou um nome de domínio do recurso da AWS, dependendo do tipo de recurso.
   - Para registros de alias que se referem a outros registros, a resposta contém um ou mais valores do registro referido.

Usar a ferramenta de verificação para simular consultas de endereços IP específicos (apenas registros de latência e localização geográfica)

Se você tiver criado registros de latência e localização geográfica, pode usar a ferramenta de verificação para simular consultas do endereço IP para um resolvedor de DNS e para um cliente.

Para usar a ferramenta de verificação para simular consultas de endereços IP especificados

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Zonas hospedadas, escolha o nome de uma zona hospedada. O console exibe a lista de registros para essa zona hospedada.
4. Para ir diretamente para a página Verificar resposta do Route 53, escolha Testar conjunto de registros.

   Para chegar à página Verificar resposta do Route 53 de um registro específico, marque a caixa de seleção daquele registro e escolha Testar conjunto de registros.
5. Se você escolher Test record set (Testar conjunto de registros) sem primeiro escolher um registro, especifique os seguintes valores:

   - O nome do registro, excluindo o nome da zona hospedada. Por exemplo, para verificar www.example.com, insira www. Para verificar example.com, deixe o campo Record name (Nome do registro) em branco.
   - O tipo de registro que você deseja verificar, como A ou CNAME.
6. Especifique os valores aplicáveis:

   Endereço IP do resolvedor

   Especifique um endereço IPv4 ou IPv6 para simular a localização do resolvedor de DNS que um cliente usa para fazer solicitações. Isso é útil para testar registros de localização geográfica e latência. Se você omitir esse valor, a ferramenta usará o endereço IP de um resolvedor de DNS na região Leste dos EUA (Norte da Virgínia) (us-east-1) da AWS.

   IP da sub-rede do cliente EDNS0

   Se o resolvedor oferecer suporte ao EDNS0, insira o IP da sub-rede do cliente de um endereço IP na localização geográfica aplicável, por exemplo, 192.0.2.0 ou 2001:db8:85a3::8a2e:370:7334.

Máscara de sub-rede

Se você especificar um endereço IP para o IP da sub-rede do cliente EDNS0, terá a opção de especificar o número de bits do endereço IP que você deseja que a ferramenta de verificação inclua na consulta de DNS. Por exemplo, se você especificar 192.0.2.44 para o IP da sub-rede do cliente EDNS0 e 24 para Máscara de sub-rede, a ferramenta de verificação de simulará uma consulta de 192.0.2.0/24. O valor padrão é 24 bits para endereços IPv4 e 64 bits para endereços IPv6.

7. Escolha Obter resposta.
8. A seção Resposta retornada pelo Route 53 inclui os seguintes valores:

Consulta de DNS enviada ao Route 53

A consulta, em formato BIND, que a ferramenta de verificação enviou ao Route 53. Este é o mesmo formato que um aplicativo web usa para enviar uma consulta. Os três valores costumam ser o nome do registro, IN (para Internet) e o tipo do registro.

Código de resposta do DNS

Um código que indica se a consulta foi válida ou não. O código de resposta mais comum é NOERROR e indica que a consulta é válida. Se a resposta não for válida, o Route 53 retornará um código de resposta que explicará o motivo. Para obter uma lista dos códigos de resposta possíveis, consulte DNS RCODES no site da IANA.

Protocolo

O protocolo que o Amazon Route 53 usou para responder a consulta. O protocolo pode ser UDP ou TCP.

Resposta retornada pelo Route 53

O valor que o Route 53 retornaria para uma aplicação Web. O valor é um dos seguintes:

- Para registros que não sejam de alias, a resposta contém um ou mais valores no registro.
- Para vários registros que têm o mesmo nome e tipo, que inclui conjuntos ponderados, de latência, localização geográfica e failover, a resposta contém o valor do registro apropriado, de acordo com a solicitação.
- Para registros de alias que fazem referência a outros recursos da AWS diferentes do registro, a resposta contém um endereço IP ou um nome de domínio do recurso da AWS, dependendo do tipo de recurso.

- Para registros de alias que se referem a outros registros, a resposta contém um ou mais valores do registro referido.

Configurar servidores de nome de rótulo branco

Cada zona hospedada do Amazon Route 53 é associada a quatro servidores de nome, conhecidos como um conjunto de delegações. Por padrão, os servidores de nome têm nomes como ns-2048.awsdns-64.com. Para que o nome do domínio de seus servidores de nome seja o mesmo nome de domínio de sua zona hospedada, por exemplo, ns1.exemplo.com, configure os servidores de nome de rótulo branco, também conhecidos como servidores de nome privado ou servidores de nome intuitivo.

As etapas a seguir explicam como configurar um conjunto de quatro servidores de nome de rótulo branco que você pode reutilizar para vários domínios. Por exemplo, suponha que você tenha os domínios exemplo.com, exemplo.org e exemplo.net. Com estas etapas, você pode configurar os servidores de nome de rótulo branco para exemplo.com e reutilizá-los para exemplo.org e exemplo.net.

Tópicos

Etapa 1: Criar um conjunto de delegações reutilizáveis do Route 53

Os servidores de nomes de rótulo branco são associados a um conjunto de delegaçõs reutilizável do Route 53. É possível usar servidores de nomes de rótulo branco para uma zona hospedada somente

se a zona hospedada e o conjunto de delegações reutilizável foram criados pela mesma conta da AWS.

Para criar um conjunto de delegações reutilizáveis, você pode usar a API do Route 53, a CLI da AWS ou um dos SDKs da AWS. Para obter mais informações, consulte a documentação a seguir:

- API do Route 53: consulte CreateReusableDelegationSet na Referência da API do Amazon Route 53
- CLI da AWS: consulte create-reusable-delegation-set na Referência de comando da AWS CLI
- SDKs da AWS: consulte a documentação do SDK aplicável na página Documentação da AWS

Etapa 2: Criar ou recriar as zonas hospedadas do Amazon Route 53 e alterar o TTL dos registros de NS e SOA

Criar ou recriar zonas hospedadas do Amazon Route 53:

- Se não estiver usando o Route 53 como o serviço DNS dos domínios para os quais você quer usar servidores de nome de rótulo branco: crie as zonas hospedadas e especifique o conjunto de delegações reutilizáveis que você criou na etapa anterior com cada zona hospedada. Para obter mais informações, consulte CreateHostedZone na Referência da API do Amazon Route 53.
- Se você estiver usando o Route 53 como o serviço DNS dos domínios para os quais você quer usar os servidores de nome de rótulo branco: crie as zonas hospedadas para as quais você quer usar os servidores de nome de rótulo branco e especifique o conjunto de delegações reutilizáveis que você criou na etapa anterior para cada zona hospedada.

> **Important**
>
> Você não pode alterar os servidores de nome associados a uma zona hospedada existente. Você pode associar um conjunto de delegações reutilizáveis a uma zona hospedada somente quando cria a zona hospedada.

Quando você criar zonas hospedadas e antes de tentar acessar os recursos dos domínios correspondente, altere os seguintes valores de TTL para cada zona hospedada:

- Altere o TTL do registro de NS da zona hospedada para 60 segundos ou menos.
- Altere o TTL mínimo do registro de SOA da zona hospedada para 60 segundos ou menos. Este é o último valor no registro de SOA.

Se, acidentalmente, você informar a seu registrador endereços IP incorretos para seus servidores de nome de rótulo branco, seu site se tornará indisponível pela duração do TTL depois que você corrigir o problema. Ao definir um TTL baixo, você reduz a quantidade de tempo que o seu site ficará indisponível.

Para obter mais informações sobre a criação de zonas hospedadas e a especificação de um conjunto de delegações reutilizáveis para os servidores de nome para as zonas hospedadas, consulte CreateHostedZone na Referência da API do Amazon Route 53.

Etapa 3: recriar registros para suas zonas hospedadas

Crie registros nas zonas hospedadas que você criou na etapa 2:

- Se estiver migrando o serviço DNS dos seus domínios para o Amazon Route 53: talvez você possa criar registros importando informações sobre seus registros existentes. Para obter mais informações, consulte Criar registros importando um arquivo de zona.
- Se você estiver substituindo zonas hospedadas existentes para que possa usar os servidores de nome de rótulo branco: as novas zonas hospedadas, recrie os registros que aparecem nas suas zonas hospedadas atuais. O Route 53 não fornece um método de exportação de registros de uma zona hospedada, mas alguns fornecedores terceirizados oferecem. Você pode usar o recurso de importação do Route 53 para importar registros que não sejam de alias para os quais a política de roteamento é simples. Não há uma maneira de exportar e reimportar registros de alias ou registros para os quais a política de roteamento não é simples.

  Para mais informações sobre a criação de registros usando a API do Route 53, consulte CreateHostedZone na Referência da API do Amazon Route 53. Para obter informações sobre como criar registros usando o console do Route 53, consulte Trabalhar com registros.

Etapa 4: obter endereços IP

Obtenha os endereços IPv4 e IPv6 dos servidores de nome no conjunto de delegações reutilizáveis e preencha na tabela a seguir.

Nome de um servidor de nome no conjunto de delegações reutilizáveis (exemplo: Ns-2048.awsdns-64.com)	Endereços IPv4 e IPv6	Nome que você deseja atribuir ao servidor de nome de rótulo branco (exemplo: ns1.exemplo.com)
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	
	IPv4: IPv6:	

Por exemplo, suponha que os quatro servidores de nome do seu conjunto de delegações reutilizáveis sejam:

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Aqui estão os comandos do Linux e do Windows que você executaria para obter os endereços IP para o primeiro dos quatro servidores de nome:

comandos dig para 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 para 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
```

Etapa 5: Criar registros para servidores de nome de rótulo branco

Na zona hospedada que tem o mesmo nome (como exemplo.com) que o nome do domínio dos servidores de nome de rótulo branco (como ns1.exemplo.com), crie oito registros:

- Um registro A para cada servidor de nome de rótulo branco
- Um registro AAAA para cada servidor de nome de rótulo branco

> **Important**
>
> Se estiver usando os mesmos servidores de nome de rótulo branco para duas ou mais zonas hospedadas, não execute essa etapa para as outras zonas hospedadas.

Para cada registro, especifique os valores a seguir. Consulte a tabela que você preencheu na etapa anterior:

Política de roteamento

Especifique Simple routing (Roteamento simples).

Nome de registro

O nome que você deseja atribuir a um dos servidores de nome de rótulo branco, por exemplo, ns1.exemplo.com. Para o prefixo (ns1 neste exemplo), você pode usar qualquer valor válido em um nome de domínio.

Valor/Encaminhar tráfego para

O endereço IPv4 ou IPv6 de um dos servidores de nome do Route 53 no conjunto de delegações reutilizáveis.

> **Important**
>
> Se você especificar endereços IP incorretos ao criar registros para os servidores de nome de rótulo branco, seu site ou aplicativo web ficará indisponível na Internet quando você executar etapas subsequentes. Mesmo que você corrija os endereços IP imediatamente, seu site ou aplicativo web permanecerá indisponível pela duração do TTL.

Tipo de registro

Especifique A quando estiver criando registros para endereços IPv4.

Especifique AAAA quando estiver criando registros para endereços IPv6.

TTL (segundos)

Este valor é a quantidade de tempo pela qual os resolvedores de DNS armazenam em cache as informações neste registro antes de encaminhar outra consulta de DNS ao Route 53. Recomendamos que você especifique um valor inicial igual ou inferior a 60 segundos. Assim, você poderá recuperar com rapidez se, acidentalmente, especificar valores incorretos nestes registros.

Etapa 6: atualizar registros de NS e SOA

Atualize os registros SOA e NS nas zonas hospedadas para as quais você deseja usar os servidores de nome de rótulo branco. Execute as etapa de 6 a 8 para uma zona hospedada e o domínio correspondente de cada vez. Em seguida, repita para outra zona hospedada e domínio.

> **Important**
>
> Comece com a zona hospedada do Amazon Route 53 que tem o mesmo nome de domínio (como example.com) que os servidores de nome de rótulo branco (como ns1.exemplo.com).

1. Atualize o registro SOA substituindo o nome do servidor de nome do Route 53 pelo nome de um de seus servidores de nome de rótulo branco

   Exemplo

   Substitua o nome do servidor de nome do Route 53:

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   pelo nome de um dos servidores de nome de rótulo branco:

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > Você alterou o último valor, a vida útil (TTL), na Etapa 2: Criar ou recriar as zonas hospedadas do Amazon Route 53 e alterar o TTL dos registros de NS e SOA.

   Para obter mais informações sobre como atualizar registros usando o console do Route 53, consulte Editar registros.
2. No registro de NS, anote os nomes dos servidores de nome atuais do domínio para que você possa reverter para esses servidores de nome se necessário.
3. Atualize o registro de NS. Substitua o nome dos servidores de nome do Route 53 pelos nomes dos quatro servidores de nome de rótulo branco, por exemplo, `ns1.example.com`, `ns2.example.com`, `ns3.example.com`, e `ns4.example.com`.

Etapa 7: criar registros cola e alterar os servidores de nome do registrador

Use o método fornecido pelo registrador para criar registros cola e alterar os servidores de nome do registrador:

1. Adicione registros cola:

   - Se estiver atualizando o domínio que tem o mesmo nome de domínio que os servidores de nome de rótulo branco: crie quatro registros cola para os quais os nomes e endereços IP correspondem aos valores que você obteve na etapa 4. Inclua os endereços IPv4 e IPv6 para um servidor de nome de rótulo branco no registro cola correspondente, por exemplo:

ns1.example.com: endereços IP = 192.0.2.117 and 2001:db8:85a3::8a2e:370:7334

Os registradores usam diversos termos para os registros cola. Os registros cola podem ser mencionados como registro de novos servidores de nome ou algo parecido.

- Se você estiver atualizando outro domínio: se o Route 53 for seu serviço DNS, primeiro você deverá concluir a etapa do marcador anterior e criar os registros cola que correspondem ao nome do domínio. Em seguida, pule para a etapa 2 deste procedimento.

2. Altere os servidores de nome do domínio para os nomes dos servidores de nome de rótulo branco.

Se estiver usando o Amazon Route 53 como o serviço DNS, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

Etapa 8: monitorar o tráfego para o site ou a aplicação

Monitore o tráfego do site ou da aplicação para os quais você criou registros cola e alterou os servidores de nome na etapa 7:

- Se o tráfego for interrompido: use o método fornecido pelo registrador para alterar os servidores de nome do domínio de volta para os servidores de nome anteriores do Route 53. Esses são os servidores de nome que você anotou na etapa 6b. Em seguida, determine o que deu errado.
- Se o tráfego não for afetado: repita as etapas 6 a 8 para as demais zonas hospedadas para as quais você quer usar os mesmos servidores de nome de rótulo branco.

Etapa 9: alterar os TTLs de volta para seus valores originais

Para todas as zonas hospedadas que agora estão usando os servidores de nome de rótulo branco, altere os seguintes valores:

- Altere o TTL do registro de NS da zona hospedada para um valor mais comum de registros de NS. Por exemplo, 172.800 segundos (dois dias).
- Altere o TTL mínimo do registro de SOA da zona hospedada para um valor mais comum de registros de SOA. Por exemplo, 900 segundos. Este é o último valor no registro de SOA.

Etapa 10: entrar em contato com serviços de DNS recursivos (opcional)

Opcional Se você estiver usando o roteamento de localização geográfica do Amazon Route 53, entre em contato com os serviços DNS recursivos que oferecem suporte à extensão edns-client-subnet do EDNS0 e forneça os nomes de seus servidores de nome de rótulo branco para eles. Isso garante que esses serviços de DNS continuarão a encaminhar as consultas de DNS para a melhor localização do Route 53 com base na localização geográfica aproximada de origem da consulta.

Registros de NS e SOA que o Amazon Route 53 cria para uma zona hospedada pública

Para cada zona hospedada pública que você cria, o Amazon Route 53 cria automaticamente um registro de servidor de nome (NS) e de início de autoridade (SOA). Raramente é necessário alterar esses registros.

Tópicos

Registro de servidor de nome (NS)

O Amazon Route 53 cria automaticamente um registro de servidor de nome (NS) que tem o mesmo nome que sua zona hospedada. Ele lista os quatro servidores de nome que são os servidores de nome autoritativos para sua zona hospedada. Exceto em circunstâncias raras, recomendamos que você não adicione, altere ou exclua servidores de nomes neste registro.

Os exemplos a seguir mostram o formato dos nomes dos servidores de nome do Route 53 (esses são apenas exemplos; não os use quando atualizar seus registros de servidor de nome do registrador):

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

Para obter a lista dos servidores de nome da sua zona hospedada:

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, clique em Hosted zones (Zonas hospedadas).
3. Na página Hosted zones (Zonas hospedadas), escolha o botão de opção (não o nome) da zona hospedada, depois escolha View details (Exibir detalhes).
4. Na página de detalhes da zona hospedada, escolha Hosted zone details (Detalhes da zona hospedada).
5. Anote os quatro servidores listados para Name servers (Servidores de nome).

Para obter informações sobre como migrar o serviço DNS de outro provedor de serviço DNS para o Route 53, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Registro de início de autoridade (SOA)

O registro de início de autoridade (SOA) identifica informações básicas de DNS sobre o domínio, por exemplo:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

Um registro SOA inclui os seguintes elementos:

- O servidor de nome do Route 53 que criou o registro SOA, por exemplo, `ns-2048.awsdns-64.net`.
- O endereço de e-mail do administrador. O símbolo `@` é substituído por um ponto, por exemplo, `hostmaster.example.com`. O valor padrão é um endereço de e-mail amazon.com que não é monitorado.
- Um número de série que você pode incrementar opcionalmente sempre que atualizar um registro na zona hospedada. O Route 53 não incrementa o número automaticamente. (O número de série é usado pelos serviços DNS que oferecem suporte a DNS secundário.) No exemplo, esse valor é `1`.
- Um tempo de atualização em segundos que os servidores DNS secundários aguardam antes de consultar o registro SOA do servidor DNS principal para verificar as alterações. No exemplo, esse valor é `7200`.

- O intervalo de repetição em segundos que um servidor secundário aguarda antes de repetir uma transferência de zona com falha. Normalmente, o tempo de repetição é menor do que o tempo de atualização. No exemplo, esse valor é `900` (15 minutos).
- O tempo de expiração em segundos que um servidor secundário continuará tentando concluir uma transferência de zona. Se esse tempo decorrer antes de uma transferência de zona bem-sucedida, o servidor secundário parará de responder a consultas porque considera que seus dados são muito antigos para serem confiáveis. No exemplo, esse valor é `1209600` (duas semanas).
- O tempo mínimo de vida (TTL). Esse valor ajuda a definir o período em que os resolvedores recursivos devem armazenar em cache as seguintes respostas do Route 53:

  NXDOMAIN

  Não há nenhum registro de qualquer tipo com o nome especificado na consulta DNS, como exemplo.com. Também não há registros que sejam filhos do nome especificado na consulta DNS, como zenith.exemplo.com.

  NODATA

  Há pelo menos um registro com o nome especificado na consulta DNS, mas nenhum desses registros tem o tipo (como A) especificado na consulta DNS.

  Quando um resolvedor DNS armazena em cache uma resposta NXDOMAIN ou NODATA, isso é conhecido como cache negativo.

  A duração do cache negativo é o menor dos seguintes valores:

  - Esse valor, o TTL mínimo no registro SOA. Na exemplo, o valor é `86400` (um dia).
  - O valor da TTL para o registro SOA. O valor de padrão é de 900 segundos. Para obter informações sobre como alterar esse valor, consulte Editar registros.

  Quando o Route 53 responde a consultas DNS com uma resposta NXDOMAIN ou NODATA (uma resposta negativa), será cobrada a taxa para consultas padrão. Consulte “Queries” (Consultas) em Preços do Amazon Route 53. Se você estiver preocupado com o custo das respostas negativas, uma opção é alterar a TTL para o registro SOA, a TTL mínima no registro SOA (esse valor) ou ambos. Observe que o aumento dessas TTLs, que se aplicam a respostas negativas para toda a zona hospedada, pode ter efeitos positivos e negativos:

  - Resolvedores DNS na Internet armazenam em cache a não existência de registros por períodos mais longos, o que reduz o número de consultas encaminhadas para o Route 53. Isso reduz a cobrança do Route 53 de consultas DNS.

- No entanto, se você excluir erroneamente um registro válido e depois recriá-lo, os resolvedores DNS armazenarão em cache a resposta negativa (esse registro não existe) por um período mais longo. Isso aumenta o tempo que seus clientes ou usuários não conseguem acessar o recurso correspondente, como um servidor web para acme.exemplo.com.

Para encontrar registros SOA no Route 53

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Selecione o nome vinculado do domínio cujos registros você deseja visualizar.
4. Na seção Records (Registros), é possível ver todos os registros listados e também filtrar registros para localizar o valor do SOA.

Trabalhar com zonas hospedadas privadas

Uma zona hospedada privada é um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs criadas com o serviço da Amazon VPC. Veja como as zonas hospedadas privadas funcionam:

1. Você cria uma zona hospedada privada, como example.com, e especifica a VPC que deseja associar a ela. Depois de criar a zona hospedada, você pode associar mais VPCs a ela.
2. Você cria registros na zona hospedada que determinam como o Route 53 responde às consultas de DNS de seu domínio e subdomínios em suas VPCs. Por exemplo, suponha que tenha um servidor de banco de dados que é executado em uma instância do EC2 na VPC que você associou à sua zona hospedada privada. Você cria um registro A ou AAAA, como db.example.com, e especifica o endereço IP do servidor de banco de dados.

   Para obter mais informações sobre registros de , consulte Trabalhar com registros. Para obter informações sobre os requisitos da Amazon VPC; para o uso de zonas hospedadas privadas, consulte Como usar zonas hospedadas privadas no Guia do usuário da Amazon VPC.
3. Quando uma aplicação enviar uma consulta de DNS db.example.com, o Route 53 retornará o endereço IP correspondente. Para obter uma resposta de uma zona hospedada privada, você também precisa estar executando uma instância do EC2 em uma das VPCs associadas (ou ter um endpoint de entrada de uma configuração híbrida). Se você tentar consultar uma zona

hospedada privada de fora das VPCs ou de sua configuração híbrida, a consulta será resolvida recursivamente na Internet.

4. A aplicação usa o endereço IP que obteve do Route 53 para estabelecer uma conexão com o servidor de banco de dados.

Quando você cria uma zona hospedada privada, os seguintes servidores de nomes são usados:

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

Esses servidores de nomes são usados porque o protocolo DNS exige que cada zona hospedada tenha um conjunto de registros de NS. Esses servidores de nomes são reservados e nunca são usados pelas zonas hospedadas públicas do Route 53. Você só pode consultar essas zonas por meio do Route 53 Resolver em uma VPC que tenha sido associada à zona hospedada usando um endpoint de entrada conectado às VPCs especificadas na zona hospedada privada.

Embora os servidores de nomes estejam visíveis na Internet, o Route 53 Resolver não se conecta aos endereços dos servidores de nomes. Além disso, as informações da zona hospedada privada não são retornadas se você consultar diretamente os servidores de nomes pela Internet. Em vez disso, o Route 53 Resolver detecta que as consultas estão dentro de um namespace privado baseado em associações de VPC para zona hospedada e usa conectividade direta e privada para acessar os servidores DNS privados.

> **Note**
>
> Você pode alterar o conjunto de registros NS em uma zona hospedada privada, se quiser, e a resolução de DNS privada ainda funcionará. Não recomendamos que você faça isso, mas se quiser, deve usar nomes de domínio reservados que não sejam usados por servidores DNS públicos.

Se você quiser encaminhar o tráfego para o seu domínio na Internet, utilize uma zona hospedada pública do Route 53. Para ter mais informações, consulte Trabalhar com zonas hospedadas públicas.

Tópicos

- Considerações ao trabalhar com uma zona hospedada privada
- Criar uma zona hospedada privada
- Listar zonas hospedadas privadas
- Associar mais VPCs a uma zona hospedada privada
- Associando uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS
- Desassociar VPCs de uma zona hospedada privada
- Excluir uma zona hospedada privada

Considerações ao trabalhar com uma zona hospedada privada

Ao usar zonas hospedadas privadas, considere o seguinte:

- 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

Configurações da Amazon VPC

Para usar zonas hospedadas privadas, é necessário definir as seguintes configurações do Amazon VPC; como `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Para obter mais informações, consulte Atualização do suporte a DNS para sua VPC no Manual do usuário da Amazon VPC.

Verificações de integridade do Route 53

Em uma zona hospedada privada, você pode associar verificações de integridade do Route 53 somente com failover, resposta de vários valores e registros ponderados, de latência e de geolocalização. Para obter informações sobre a associação de verificações de integridade com registros de failover, consulte Configurar failover em uma zona hospedada privada.

Políticas de roteamento com suporte para registros em uma zona hospedada privada

Você pode usar as seguintes políticas de roteamento ao criar registros em uma zona hospedada privada:

- Roteamento simples
- Roteamento de failover
- Roteamento de resposta com vários valores
- Roteamento ponderado
- Roteamento baseado em latência
- Roteamento de localização geográfica
- Roteamento por geoproximidade

Não há suporte para a criação de registros em uma zona hospedada privada usando outras políticas de roteamento.

DNS com exibição segmentada

É possível usar o Route 53 para configurar o DNS com exibição segmentada, também conhecido como DNS com horizonte segmentado. No DNS com exibição segmentada, você usa o mesmo nome de domínio (example.com) para usos internos (accounting.example.com) e para usos externos, como seu site público (www.example.com). Você também pode usar o mesmo nome de subdomínio interna e externamente, mas fornecer conteúdo diferente ou exigir autenticação diferente para usuários internos e externos.

Para configurar o DNS com exibição segmentada, execute as seguintes etapas:

1. Crie zonas hospedadas públicas e privadas que tenham o mesmo nome. (O DNS com exibição segmentada ainda funcionará se você estiver usando outro serviço de DNS para a zona hospedada pública.)
2. Associe uma ou mais Amazon VPCs à zona hospedada privada. O Route 53 Resolver usa a zona hospedada privada para encaminhar consultas de DNS nas VPCs especificadas.

3. Crie registros em cada zona hospedada. Os registros na zona hospedada pública controlam como o tráfego da Internet é roteado, e os registros na zona hospedada privada controlam como o tráfego é roteado nas suas Amazon VPCs.

Se precisar executar a resolução de nomes de sua VPC e de workloads on-premises, você poderá usar o Route 53. Para ter mais informações, consulte O que Amazon Route 53 Resolveré.

Zonas hospedadas públicas e privadas que têm namespaces sobrepostos

Se você tiver zonas hospedadas privadas e públicas que tenham namespaces sobrepostos, como example.com e accounting.example.com, o Resolver encaminhará o tráfego com base na correspondência mais específica. Quando os usuários estão conectados a uma instância do EC2 em uma Amazon VPC que você associou à zona hospedada privada, veja como Route 53 Resolver lida com consultas DNS:

1. O Resolver avaliará se o nome da zona hospedada privada corresponde ao nome de domínio na solicitação, por exemplo, accounting.example.com. Uma correspondência é definida como uma das seguintes opções:
   - Correspondência idêntica
   - O nome da zona hospedada privada é pai do nome de domínio na solicitação. Por exemplo, suponhamos que o nome de domínio na solicitação seja o seguinte:

     seattle.accounting.example.com

     As zonas hospedadas a seguir serão correspondentes porque são pais de seattle.accounting.example.com:
     - accounting.example.com
     - example.com

   Se não houver uma zona hospedada privada correspondente, o Resolver encaminhará a solicitação a um resolvedor de DNS público. Depois, sua solicitação será resolvida como uma consulta de DNS normal.
2. Se houver um nome de zona hospedada privada que corresponda ao nome de domínio na solicitação, será pesquisado na zona hospedada um registro que corresponda ao nome de domínio e ao tipo de DNS na solicitação, por exemplo, um registro A para accounting.example.com.

> **Note**
>
> Se houver uma zona hospedada privada correspondente, mas não um registro que corresponda ao nome e ao tipo do domínio na solicitação, o Resolver não encaminhará a solicitação para um resolvedor de DNS público. Em vez disso, ele retornará NXDOMAIN (domínio inexistente) para o cliente.

Zonas hospedadas privadas que têm namespaces sobrepostos

Se você tiver uma ou mais zonas hospedadas privadas com namespaces sobrepostos, tais como example.com e accounting.example.com, o Resolver encaminhará o tráfego com base na correspondência mais específica.

> **Note**
>
> Se você tiver uma zona hospedada privada (example.com) e uma regra do Route 53 Resolver que encaminha o tráfego para a rede, para o mesmo nome de domínio, a regra do Resolver terá precedência. Consulte Private hosted zones and Route 53 Resolver rules.

Quando os usuários estiverem conectados a uma instância do EC2 em uma Amazon VPC que você associou a todas as zonas hospedadas privadas, veja como o Resolver lida com consultas DNS:

1. O Resolver avalia se o nome de domínio na solicitação, por exemplo, accounting.example.com, corresponde ao nome de uma das zonas hospedadas privadas.
2. Se não houver uma zona hospedada que corresponda exatamente ao nome de domínio na solicitação, o Resolver buscará uma zona hospedada que tenha um nome que seja pai do nome de domínio na solicitação. Por exemplo, suponhamos que o nome de domínio na solicitação seja o seguinte:

   `seattle.accounting.example.com`

   As zonas hospedadas a seguir são correspondentes porque são pais de `seattle.accounting.example.com`:

   - `accounting.example.com`
   - `example.com`

O Resolver escolhe o `accounting.example.com` porque é mais específico que `example.com`.

3. O Resolver procura um registro na zona hospedada `accounting.example.com` que corresponda ao nome de domínio e ao tipo de DNS na solicitação, como um registro A para `seattle.accounting.example.com`.

   Se não houver registros que correspondam ao nome e ao tipo de domínio na solicitação, o Resolver retornará NXDOMAIN (domínio não existente) para o cliente.

Zonas hospedadas privadas e regras do Route 53 Resolver

Se você tiver uma zona hospedada privada (example.com) e uma regra do Resolver que encaminha o tráfego para a rede, para o mesmo nome de domínio, a regra do Resolver terá precedência.

Por exemplo, suponha que você tenha a seguinte configuração:

- Você tem uma zona hospedada privada chamada example.com e a associa a uma VPC.
- Você cria uma regra do Route 53 Resolver que encaminha o tráfego para example.com para sua rede e associa a regra com a mesma VPC.

Nessa configuração, a regra do Resolver tem precedência sobre a zona hospedada privada. As consultas DNS são encaminhadas para a rede em vez de serem resolvidas com base nos registros na zona hospedada privada.

Delegar responsabilidade para um subdomínio

Não é possível criar registros NS em uma zona hospedada privada para delegar responsabilidade de um subdomínio.

Servidores DNS personalizados

Se você configurou servidores DNS personalizados nas instâncias do Amazon EC2 na sua VPC, terá que configurar esses servidores DNS para encaminhar suas consultas de DNS privadas para o endereço IP dos servidores DNS fornecidos pela Amazon para a sua VPC. Esse endereço IP é o endereço IP na base do intervalo de rede da VPC "mais dois". Por exemplo, se o intervalo CIDR da sua VPC for 10.0.0.0/16, o endereço IP do servidor DNS será 10.0.0.2.

Se quiser encaminhar consultas de DNS entre VPCs e sua rede, você poderá usar o Resolver. Para ter mais informações, consulte O que Amazon Route 53 Resolveré.

Permissões obrigatórias do IAM

Para criar zonas hospedadas privadas, é necessário conceder permissões ao IAM para ações do Amazon EC2, além das permissões para ações do Route 53. Para obter mais informações, consulte Ações, recursos e chaves de condição do Route 53 na Referência de autorização do serviço.

Criar uma zona hospedada privada

Uma zona hospedada privada é um contêiner para registros de um domínio que você hospeda em uma ou mais nuvens privadas virtuais (VPCs) da Amazon. Você cria uma zona hospedada para um domínio (como example.com) e depois cria registros para informar ao Amazon Route 53 como você quer que o tráfego seja encaminhado para esse domínio nas suas VPCs.

Important

Ao criar uma zona hospedada privada, é necessário associar uma VPC a ela. Além disso, a VPC especificada precisa ter sido criada usando a mesma conta que você está usando para criar a zona hospedada. Depois de criar a zona hospedada, você pode associar VPCs adicionais a ela, incluindo VPCs que você criou usando uma conta diferente AWS .
Para associar VPCs criadas com uma conta a uma zona hospedada privada criada com outra conta, é necessário autorizar essa associação e realizá-la programaticamente. Para ter mais informações, consulte Associando uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS.

Para obter informações sobre como criar uma zona hospedada privada usando a API do Route 53, consulte a Referência da API do Amazon Route 53.

Para criar uma zona hospedada privada usando o console do Route 53

1. Em cada VPC que você quer associar à zona hospedada do Route 53, altere as seguintes configurações da VPC para `true`:
   - `enableDnsHostnames`
   - `enableDnsSupport`

Para obter mais informações, consulte Atualização do suporte a DNS para sua VPC no Manual do usuário da Amazon VPC.

2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. Se você for novo no Route 53, escolha Get started (Conceitos básicos)

   Se você já estiver usando o Route 53, escolha Hosted zones (Zonas hospedadas) no painel de navegação.
4. Escolha Create hosted zone (Criar zona hospedada).
5. No painel Create private hosted zone (Criar zona hospedada privada), insira um nome de domínio e, se quiser, um comentário.

   Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.
6. Na lista Type (Tipo), escolha Private Hosted Zone (Zona hospedada privada).
7. Na lista ID da VPC, escolha a VPC que você deseja associar à zona hospedada.

   > **Note**
   >
   > Se o console exibir a seguinte mensagem, significa que você está tentando associar uma zona hospedada que usa o mesmo namespace que o de outra zona hospedada na mesma VPC:
   > "Um domínio conflitante já está associado à VPC ou ao conjunto de delegação especificado".
   > Por exemplo, se a zona hospedada A e a zona B hospedadas tiverem o mesmo nome de domínio, por exemplo `example.com`, você não poderá associar ambas as zonas hospedadas à mesma VPC.
8. Escolha Create hosted zone (Criar zona hospedada).

Listar zonas hospedadas privadas

Você pode usar o console do Amazon Route 53 para listar todas as zonas hospedadas que você criou com a AWS conta atual. Para obter informações sobre como listar zonas hospedadas usando a API do Route 53, consulte ListHostedZonas na referência da API do Amazon Route 53.

Para listar as zonas hospedadas associadas a uma AWS conta

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

   A página Zonas hospedadas exibe automaticamente uma lista de todas as zonas hospedadas que foram criadas usando a AWS conta atual. A coluna Tipo indica se a zona hospedada é privada ou pública. Escolha o cabeçalho da coluna para agrupar todas as zonas hospedadas privadas e públicas.

Associar mais VPCs a uma zona hospedada privada

Você pode usar o console do Amazon Route 53 para associar mais VPCs a uma zona hospedada privada se tiver criado a zona hospedada e as VPCs usando a mesma AWS conta.

> **Important**
>
> Se quiser associar VPCs criadas com uma conta a uma zona hospedada privada criada com outra conta, é necessário autorizar essa associação. Além disso, não é possível usar o console da AWS para autorizar a associação ou associar as VPCs à zona hospedada. Para ter mais informações, consulte Associando uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS.

Para obter informações sobre como associar mais VPCs a uma zona hospedada privada usando a API do Route 53, consulte AssociateVPC Zone WithHosted na Amazon Route 53 API Reference.

Para associar outras VPCs a uma zona hospedada privada usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

3. Escolha o botão de opção da zona hospedada privada à qual você deseja associar mais VPCs.
4. Selecione a opção Editar.
5. Escolha Add VPC (Adicionar VPC)
6. Escolha a região e o ID da VPC que você quer associar a esta zona hospedada.
7. Para associar mais VPCs a essa zona hospedada, repita as etapas 5 e 6.
8. Escolha Salvar alterações.

Associando uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS

Se você quiser associar uma VPC criada a uma AWS conta a uma zona hospedada privada criada com uma conta diferente, execute o procedimento a seguir:

Para associar uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS

1. Usando a conta com a qual você criou a zona hospedada, autorize a associação da VPC à zona hospedada privada de uma destas formas:

   - AWS CLI: consulte create-vpc-association-authorization na Referência de comando da AWS CLI
   - AWS SDK ou AWS Tools for Windows PowerShell— Consulte a documentação aplicável na página de AWS documentação
   - API do Amazon Route 53 — Consulte CreateVPC AssociationAuthorization na referência da API do Amazon Route 53

   Observe o seguinte:

   - Se você quiser associar várias VPCs criadas com uma conta a uma zona hospedada criada com outra conta, será necessário enviar uma solicitação de autorização para cada VPC.
   - Ao autorizar a associação, você precisa especificar o ID da zona hospedada. Por isso, a zona hospedada privada deve ser existente.
   - Não é possível usar o console do Route 53 para realizar ou autorizar a associação de uma VPC à zona hospedada privada.

2. Usando a conta com a qual a VPC foi criada, associe a VPC à zona hospedada. Assim como na autorização da associação, você pode usar o AWS SDK, o Tools for Windows PowerShell ou a AWS CLI API do Route 53. Se você estiver usando a API, use a ação AssociateVPC WithHosted Zone.
3. Recomendado: exclua a autorização para associar a VPC à zona hospedada. Excluir a autorização não afeta a associação. Isso apenas evita que você associe a VPC à zona hospedada novamente. Se quiser reassociar a VPC à zona hospedada, repita as etapas 1 e 2 deste procedimento.

> **Note**
>
> Para ver o número máximo de autorizações que podem ser criadas, consulte Cotas em entidades.

Desassociar VPCs de uma zona hospedada privada

Você pode usar o console do Amazon Route 53 para desassociar VPCs de uma zona hospedada privada. Isso faz com que o Route 53 interrompa o tráfego de roteamento usando registros na zona hospedada para consultas DNS originadas na VPC. Por exemplo, se a zona hospedada example.com estiver associada a uma VPC e você desassociar a zona hospedada dessa VPC, o Route 53 parará de resolver consultas DNS para example.com ou qualquer um dos outros registros na zona hospedada example.com.

> **Note**
>
> Não é possível desassociar a última VPC de uma zona hospedada privada. Se você quiser desassociar essa VPC, primeiro deverá associar outra VPC à zona hospedada.

Para desassociar VPCs de uma zona hospedada privada

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha o botão de opção da zona hospedada privada da qual você quer desassociar uma ou mais VPCs.

4. Selecione a opção Editar.
5. Escolha Remove VPC (Remover VPC) ao lado da VPC que você quer desassociar dessa zona hospedada.
6. Escolha Salvar alterações.

Excluir uma zona hospedada privada

Esta seção explica como excluir uma zona hospedada privada usando o console do Amazon Route 53.

Você só pode excluir uma zona hospedada privada se não houver outros registros que não sejam os registros padrão de SOA e de NS. Se a sua zona hospedada contiver outros registros, você precisará excluí-los antes de excluir a zona hospedada. Isso evita que você exclua acidentalmente uma zona hospedada que ainda contém registros.

Tópicos

Excluir zonas hospedadas privadas que foram criadas por outro serviço

Se uma zona hospedada privada foi criada por outro serviço, você não pode excluí-la usando o console do Route 53. Em vez disso, você precisa usar o processo aplicável para outros serviços:

- AWS Cloud Map— Para excluir uma zona hospedada AWS Cloud Map criada quando você criou um namespace DNS privado, exclua o namespace. AWS Cloud Map exclui a zona hospedada automaticamente. Para obter mais informações, consulte Deleting namespaces (Excluir namespaces) no AWS Cloud Map Guia do desenvolvedor.
- Descoberta de serviço do Amazon Elastic Container Service (Amazon ECS): para excluir uma zona hospedada privada que o Amazon ECS criou quando você criou um serviço usando a descoberta de serviço, exclua os serviços do Amazon ECS que estão usando o namespace e exclua o namespace. Para obter mais informações, consulte Como excluir um serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

Como usar o console do Route 53 para excluir uma zona hospedada privada

Para usar o console do Route 53 para excluir uma zona hospedada privada, execute o procedimento a seguir.

Para excluir uma zona hospedada privada usando o console do Route 53.

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Verifique se a zona hospedada que você deseja excluir contém apenas um registro NS e SOA. Se houver registros adicionais nas zonas hospedadas, exclua-os:
   a. Escolha o nome da zona hospedada que você deseja excluir.
   b. Na página Record (Registro), se a lista de registros incluir quaisquer registros para os quais o valor da coluna Tipo for diferente de NS ou SOA, escolha a linha e Delete (Excluir).

      Para selecionar vários registros consecutivos, escolha a primeira linha, mantenha a tecla Shift pressionada e selecione a última linha. Para selecionar vários registros não consecutivos, escolha a primeira linha, mantenha a tecla Ctrl pressionada e selecione as demais linhas.
3. Na página Zonas hospedadas, escolha a linha da zona hospedada que você deseja excluir.
4. Escolha Excluir.
5. Digite a chave de confirmação e escolha Delete (Excluir).

Migrando uma zona hospedada para uma conta diferente AWS

Se quiser migrar uma zona hospedada de uma AWS conta para outra, você pode listar programaticamente os registros na zona hospedada antiga, editar a saída e, em seguida, criar registros programaticamente em uma nova zona hospedada usando a saída editada. Observe o seguinte:

- Se tiver apenas alguns registros, você também poderá usar o console do Route 53 para criar registros na nova zona hospedada. Para ter mais informações, consulte Criar registros usando o console do Amazon Route 53.
- Alguns procedimentos usam o AWS Command Line Interface (AWS CLI). Você também pode realizar esses procedimentos usando um dos AWS SDKs, a API do Amazon Route 53 ou AWS

Tools for Windows PowerShell. Para este tópico, usamos o AWS CLI porque é mais fácil para um pequeno número de zonas hospedadas.

- Você também pode usar esse processo para criar registros em uma nova zona hospedada com um nome diferente dos nomes de zonas hospedadas existentes, mas que tenha os mesmos registros.
- Não é possível migrar registros de alias que roteiam o tráfego para instâncias de política de tráfego.

Tópicos

Etapa 1: instalar ou atualizar o AWS CLI

Para obter informações sobre como baixar, instalar e configurar o AWS CLI, consulte o Guia do AWS Command Line Interface usuário.

> **Note**
>
> Configure a CLI de forma que você possa usá-la quando estiver usando tanto a conta que criou a zona hospedada quanto a conta para onde está migrando a zona hospedada. Para obter mais informações, consulte Configurar no Guia do usuário da AWS Command Line Interface .

Se você já estiver usando o AWS CLI, recomendamos que você atualize para a versão mais recente da CLI para que os comandos da CLI suportem os recursos mais recentes do Route 53.

Etapa 2: criar uma nova zona hospedada

O procedimento a seguir explica como usar o console do Route 53 para criar a zona hospedada para onde você quer migrar.

> **Note**
>
> O Route 53 atribui um novo conjunto de quatro servidores de nome à nova zona hospedada. Depois de migrar uma zona hospedada para outra AWS conta, você precisa atualizar o registro do domínio para usar os servidores de nomes da nova zona hospedada. Lembraremos você sobre esta etapa posteriormente no processo.

Para criar a nova zona hospedada usando uma conta diferente

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Faça login com as credenciais da conta para a qual você deseja migrar a zona hospedada.
2. Crie uma zona hospedada. Para ter mais informações, consulte Criar uma zona hospedada pública.
3. Anote o ID da zona hospedada. Em alguns casos, você precisará dessa informação mais adiante no processo.
4. Faça logout do console do Route 53.

Etapa 3: criar um arquivo que contém os registros que você deseja migrar

Para migrar registros de uma zona hospedada para outra, crie um arquivo contendo os registros que deseja migrar, edite o arquivo e, em seguida, use o arquivo editado para criar os registros na nova zona hospedada. Execute o procedimento a seguir para criar o arquivo.

Para criar um arquivo contendo os registros que você deseja migrar

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

Faça login com as credenciais da conta que criou a zona hospedada que você deseja migrar.

2. Obtenha o ID da zona hospedada que você deseja migrar:

   a. No painel de navegação, escolha Zonas hospedadas.

   b. Localize a zona hospedada que você deseja migrar. Se você tiver muitas zonas hospedadas, você pode escolher Exact domain name (Nome de domínio exato) e inserir o nome da zona hospedada e pressionar Enter para filtrar a lista.

   c. Obtenha o valor da coluna Hosted zone ID (ID da zona hospedada).

3. Execute o seguinte comando:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

   Observe o seguinte:

   - Para *hosted-zone-id*, especifique o ID da zona hospedada que você obteve na etapa 2 deste procedimento.
   - Para *path-to-output-file*, especifique o caminho do diretório e o nome do arquivo em que você deseja salvar a saída.
   - O caractere > envia a saída para o arquivo especificado.
   - O manipula AWS CLI automaticamente a paginação para zonas hospedadas que contêm mais de 100 registros. Para obter mais informações, consulte Usando as opções de paginação da interface de linha de AWS comando no Guia do AWS Command Line Interface usuário.

     Se você usar outro método programático para listar registros, como um dos AWS SDKs, poderá obter no máximo 100 registros por página de resultados. Se a zona hospedada contiver mais de 100 registros, você terá que enviar várias solicitações para listar todos os registros.
   - Para executar o comando em versões do Windows PowerShell anteriores à 6.0, use a seguinte sintaxe:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
```

Por exemplo, se você estiver executando o AWS CLI em um computador Windows, poderá executar o seguinte comando:

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp
\list-records-ZOLDZONE12345.txt
```

Se você estiver executando o AWS CLI em um computador Windows em uma versão do Windows PowerShell anterior à 6.0, você pode executar o seguinte comando:

```
$output = aws route53 list-resource-record-sets --hosted-zone-id <hosted-zone-id>;
 $mypath = <output-path ;
[System.IO.File]::WriteAllLines($mypath,$output)
```

4. Faça uma cópia dessa saída. Depois de criar registros na nova zona hospedada, recomendamos que você execute o AWS CLI `list-resource-record-sets` comando na nova zona hospedada e compare as duas saídas para garantir que todos os registros foram criados.

Etapa 4: editar os registros que você deseja migrar

O formato do arquivo que você criou no procedimento anterior é próximo ao formato exigido pelo AWS CLI `change-resource-record-sets` comando usado para criar registros na nova zona hospedada. No entanto, o arquivo requer algumas edições. Você deverá aplicar algumas alterações em todos os registros. Você pode fazer essas alterações usando a função de pesquisa e substituição em um bom editor de texto.

Abra uma cópia do arquivo que você criou em Etapa 3: criar um arquivo que contém os registros que você deseja migrare faça as seguintes alterações:

- Exclua as duas primeiras linhas na parte superior da saída:

```
{
    "ResourceRecordSets": [
```

- Exclua as linhas relacionadas aos registros de NS e de SOA. A nova zona hospedada já tem esses registros.
- Opcional: adicione um elemento `Comment`.

- Adicione um elemento `Changes`.
- Para cada registro, adicione uma `Action` e um elemento `ResourceRecordSet`.
- Adicione as chaves de abrir e fechar (`{ }`), conforme necessário para tornar o código JSON válido.

> **Note**
>
> Você pode usar um validador JSON para verificar se todas as chaves e colchetes estão nos locais corretos. Para encontrar um validador JSON online, realize uma pesquisa na Internet com "`json validator`".

- Se a zona hospedada contiver algum alias que faça referência a outros registros na mesma zona hospedada, faça as seguintes alterações:
  - Altere o ID da zona hospedada para o ID da nova zona hospedada.

    > **Important**
    >
    > Se o registro de alias estiver apontando para outro recurso, por exemplo, um balanceador de carga, não altere o ID da zona hospedada para o ID da zona hospedada do próprio recurso, não o ID da zona hospedada do domínio. Se você alterar a ID da zona hospedada acidentalmente, reverta a ID da zona hospedada para a ID da zona hospedada do próprio recurso, não para a ID da zona hospedada do domínio. Esse ID da zona hospedada pode ser encontrado no AWS console em que o recurso foi criado.

  - Mova os registros de alias para a parte inferior do arquivo. O Route 53 deve criar o registro ao qual um registro de alias se refere antes de criar o registro de alias.

    > **Important**
    >
    > Se um ou mais registros de alias se referem a outros registros de alias, os registros que são o destino do alias devem aparecer no arquivo antes dos registros de alias que fazem a referência. Por exemplo, se `alias.example.com` for o destino de alias para `alias.alias.example.com`, `alias.example.com` deve aparecer primeiro no arquivo.

  - Exclua os registros de alias que roteiam o tráfego para uma instância de política de tráfego. Anote os registros para que você possa recriá-los posteriormente.

- Você pode usar esse processo para criar registros em uma zona hospedada com um nome diferente. Para cada registro na saída, altere a parte do nome de domínio do elemento `Name` para o nome da nova zona hospedada. Por exemplo, se você lista os registros na zona hospedada example.com e deseja criar registros em uma zona hospedada example.net, altere a parte example.com do nome de cada registro para example.net:

  From:

  - `"Name": "example.com."`
  - `"Name": "www.example.com."`

  Para:

  - `"Name": "example.net."`
  - `"Name": "www.example.net."`

O exemplo a seguir mostra a versão editada dos registros de uma zona hospedada para example.com. O texto em itálico vermelho, é novo:

```
{
    "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."
            }
        }
    ]
}
```

Etapa 5: dividir os arquivos grandes em arquivos menores

Se você tiver uma grande quantidade de registros ou se tiver registros que têm uma grande quantidade de valores (por exemplo, uma grande quantidade de endereços IP), pode ser necessário dividir o arquivo em arquivos menores. Estes são os máximos:

- Cada arquivo pode ter um máximo de 1.000 registros.
- O tamanho máximo combinado dos valores em todos os elementos `Value` é de 32.000 bytes.

Etapa 6: criar registros na nova zona hospedada

Para criar registros na nova zona hospedada, use o seguinte 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
```

Por exemplo: .

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch
 file://c:/temp/change-records-ZNEWZONE1245.txt
```

Se você tiver excluído os registros de alias que encaminham o tráfego para uma instância de política de tráfego, recrie-os usando o console do Route 53. Para ter mais informações, consulte Criar registros usando o console do Amazon Route 53.

Etapa 7: comparar registros das zonas hospedadas nova e antiga

Para confirmar que você criou com êxito todos os registros na nova zona hospedada, recomendamos que você liste os registros na nova zona hospedada e compare a saída com a lista de registros da antiga zona hospedada. Para fazer isso, execute o procedimento a seguir.

Para comparar registros das zonas hospedadas nova e antiga

1. Execute o seguinte comando:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json
    > path-to-output-file
   ```

   Especifique os seguintes valores:

   - Para *hosted-zone-id*, especifique o ID da nova zona hospedada.
   - Para *path-to-output-file*, especifique o caminho do diretório e o nome do arquivo em que você deseja salvar a saída. Use um nome de arquivo que seja diferente do nome do arquivo que você usou em Etapa 3: criar um arquivo que contém os registros que você deseja migrar. Ao usar um nome de arquivo diferente, você garante que o arquivo novo não substituirá o arquivo antigo.
   - O caractere > envia a saída para o arquivo especificado.

   Por exemplo, se você estiver usando um computador com o Windows, poderá executar o seguinte comando:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json
    > c:\temp\list-records-ZNEWZONE67890.txt
   ```

2. Compare a saída obtida com a saída de Etapa 3: criar um arquivo que contém os registros que você deseja migrar.

   A não ser pelos valores dos registros de NS e de SOA e por todas as alterações feitas em Etapa 4: editar os registros que você deseja migrar (como IDs de zona hospedada ou nomes de domínio diferentes), as duas saídas devem ser idênticas.

3. Se os registros na nova zona hospedada não correspondem aos registros na antiga zona hospedada, você pode realizar uma das seguintes ações:

- Faça pequenas correções usando o console do Route 53. Para ter mais informações, consulte Editar registros.
- Se houver um grande número de registros ausentes, crie um novo arquivo de texto contendo os registros ausentes e, em seguida, repita Etapa 6: criar registros na nova zona hospedada.
- Exclua todos os registros, exceto os registros de NS e de SOA, da nova zona hospedada e repita as etapas a seguir:
  - Etapa 4: editar os registros que você deseja migrar
  - Etapa 5: dividir os arquivos grandes em arquivos menores
  - Etapa 6: criar registros na nova zona hospedada
  - Etapa 7: comparar registros das zonas hospedadas nova e antiga

Etapa 8: atualizar o registro do domínio para usar servidores de nome para a nova zona hospedada

Ao concluir a criação de registros na nova zona hospedada, altere os servidores de nome do registro do domínio para usarem os servidores de nome da nova zona hospedada.

> **Important**
>
> Se você não atualizar o registro do domínio para usar os servidores de nome da nova zona hospedada, o Route 53 continuará usando a zona hospedada antiga para encaminhar o tráfego para o domínio. Se você excluir a zona hospedada antiga sem atualizar os servidores de nome do registro do domínio, o domínio ficará indisponível na Internet. Se você adicionar, atualizar ou excluir registros na nova zona hospedada sem atualizar os servidores de nome do registro do domínio, o tráfego não será roteado com base nessas alterações.

Para ter mais informações, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

> **Note**
>
> Se você usar o processo para migrar o serviço DNS para um domínio que está em uso ou o processo para um domínio inativo, poderá ignorar as etapas a seguir, pois já criou uma nova zona hospedada e os registros na zona hospedada:

- Etapa 1: obter a configuração DNS atual do provedor de serviço de DNS atual
- Etapa 2: criar uma zona hospedada
- Etapa 3: criar registros

Etapa 9: aguardar os resolvedores DNS começarem a usar a nova zona hospedada

Se seu domínio estiver em uso, por exemplo, se os usuários estiverem usando o nome de domínio para navegar em um site ou acessar uma aplicação Web, os resolvedores DNS terão armazenado em cache os nomes dos servidores de nomes que foram fornecidos por seu provedor de serviço DNS atual. Um resolvedor DNS que armazenou essas informações em cache há alguns minutos irá salvá-los por até dois dias.

> **Note**
>
> Se você tiver criado registros na nova zona hospedada que não aparecem na zona hospedada antiga, os usuários não poderão usar os novos registros para acessar seus recursos até que os resolvedores comecem a usar os servidores de nome da nova zona hospedada. Por exemplo, suponha que você crie um registro, teste.exemplo.com, na nova zona hospedada que deve rotear o tráfego de Internet para seu site. Se o registro não aparecer na zona hospedada antiga, você não poderá inserir teste.exemplo.com em um navegador da Web até que os resolvedores comecem a usar a nova zona hospedada.

Para garantir que a migração de uma zona hospedada para outra AWS conta tenha sido concluída antes de excluir a zona hospedada antiga, aguarde dois dias após atualizar o registro do domínio para usar servidores de nomes para a nova zona hospedada. Após o TTL de dois dias expirar e os resolvedores solicitarem os servidores de nome de seu domínio, os resolvedores obterão os servidores de nome atuais. Você também pode habilitar Log de consultas do Resolver para monitorar consultas nas novas zonas hospedadas. Para obter informações sobre os preços do registro de consultas do Resolver, consulte CloudWatch preços.

Etapa 10: (opcional) excluir a zona hospedada antiga

Opcionalmente, quando você estiver certo de que não precisa mais da zona hospedada antiga, poderá excluí-la.

> **Important**
>
> Não exclua a zona hospedada antiga ou quaisquer registros nessa zona hospedada por pelo menos 48 horas depois de atualizar o registro do domínio para usar servidores de nome da nova zona hospedada. Se você excluir a zona hospedada antiga antes dos resolvedores DNS pararem de usar os registros nessa zona hospedada, seu domínio poderá estar indisponível na Internet até que os resolvedores comecem a usar a nova zona hospedada.

A zona hospedada deve estar vazia, com exceção dos registros de NS e SOA padrão. Se a antiga zona hospedada contém uma grande quantidade de registros, excluí-los usando o console pode levar muito tempo. Uma opção é executar as etapas a seguir:

1. Faça uma cópia do arquivo editado a partir de Etapa 4: editar os registros que você deseja migrar.
2. Na cópia do arquivo, altere `"Action": "CREATE"` para `"Action": "DELETE"` em todos os registros.
3. Use o AWS CLI comando a seguir para excluir os registros:

   ```
   aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --
   change-batch file:///path-to-file-that-contains-records
   ```

   > **Important**
   >
   > Certifique-se de que o valor especificado para o ID da zona hospedada é o ID da zona hospedada antiga, e não o ID da zona hospedada nova.

4. Exclua todos os demais registros e a zona hospedada:

   a. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

      Faça login com as credenciais da conta que criou a zona hospedada antiga.

   b. No painel de navegação, escolha Zonas hospedadas.

   c. Escolha o nome da zona hospedada antiga. Se você tiver muitas zonas hospedadas, você pode escolher Exact domain name (Nome de domínio exato) e inserir o nome da zona hospedada e pressionar Enter para filtrar a lista.

d. Se a zona hospedada contiver algum registro que não seja um registro padrão de NS e SOA (como registros de alias que encaminham o tráfego para uma instância de política de tráfego), marque as caixas de seleção correspondentes e escolha Delete (Excluir).

e. No painel de navegação, escolha Zonas hospedadas.

f. Na lista de zonas hospedadas, escolha o botão de opção da zona hospedada que você deseja excluir.

g. Escolha Excluir.

Trabalhar com registros

Depois de criar uma zona hospedada para seu domínio, como exemplo.com, você cria registros para informar ao Domain Name System (DNS) como deseja que o tráfego seja roteado para esse domínio.

Por exemplo, você pode criar registros que fazem com que o DNS faça o seguinte:

- Roteie tráfego de Internet de exemplo.com para o endereço IP de um host no seu datacenter.
- Roteie e-mail desse domínio (ichiro@exemplo.com) para um servidor de e-mail (mail.exemplo.com).
- Roteie o tráfego de um subdomínio chamado operacoes.toquio.exemplo.com para o endereço IP de um host diferente.

Cada registro inclui o nome de um domínio ou subdomínio, um tipo de registro (por exemplo, um registro com um tipo MX roteia o e-mail) e outras informações aplicáveis ao tipo de registro (para registros MX, o nome de host de um ou mais servidores de e-mail e uma prioridade para cada servidor). Para obter informações sobre os tipos diferentes de registros, consulte Tipos de registro de DNS com suporte.

O nome de cada registro em uma zona hospedada deve terminar com o nome da zona hospedada. Por exemplo, a zona hospedada exemplo.com pode conter registros dos subdomínios www.exemplo.com e contabilidade.toquio.exemplo.com, mas não pode conter registros de um subdomínio www.exemplo.ca.

> **Note**
>
> Para criar registros para configurações de roteamento complexas, você também pode usar o editor visual de fluxo de tráfego e salvar a configuração como uma política de tráfego. Em seguida, é possível associar a política de tráfego a um ou mais nomes de domínio (como example.com) ou nomes de subdomínio (como www.example.com), na mesma ou em várias zonas hospedadas. Além disso, você poderá reverter as atualizações se a nova configuração não estiver sendo executada conforme o esperado. Para ter mais informações, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS.

O Amazon Route 53 não cobra pelos registros que você adiciona a uma zona hospedada. Para obter informações sobre o número máximo de registros que podem ser criados em uma zona hospedada, consulte Cotas.

Tópicos

Escolher uma política de roteamento

Quando você cria um registro, é possível escolher uma política de roteamento, o que determina como o Amazon Route 53 responde a consultas:

- Simple routing policy (Política de roteamento simples): use para um único recurso que executa uma determinada função para seu domínio, por exemplo, um servidor Web que oferece conteúdo

para o site example.com. Você pode usar roteamento simples para criar registros em uma zona hospedada privada.

- Failover routing policy (Política de roteamento de failover): use quando quiser configurar o failover ativo-passivo. Você pode usar roteamento com failover para criar registros em uma zona hospedada privada.
- Geolocation routing policy (Política de roteamento de localização geográfica): use quando quiser encaminhar o tráfego com base na localização dos usuários. Você pode usar roteamento por geolocalização para criar registros em uma zona hospedada privada.
- Política de roteamento por geoproximidade: use quando quiser rotear o tráfego de acordo com a localização dos recursos e, opcionalmente, mudar o tráfego dos recursos em um local para os recursos em outro local. Você pode usar o roteamento por geoproximidade para criar registros em uma zona hospedada privada.
- Política de roteamento de latência — Use quando você tiver vários recursos Regiões da AWS e quiser rotear o tráfego para a região que fornece a melhor latência. Você pode usar roteamento por latência para criar registros em uma zona hospedada privada.
- IP-based routing policy (Política de roteamento baseado em IP): use quando quiser rotear o tráfego com base no local dos usuários e tiver os endereços IP de origem do tráfego.
- Multivalue answer routing policy (Política de roteamento de resposta com vários valores): use quando quiser que o Route 53 responda a consultas de DNS com até oito registros íntegros selecionados aleatoriamente. Você pode usar roteamento com resposta multivalor para criar registros em uma zona hospedada privada.
- Weighted routing policy (Política de roteamento ponderado): use para encaminhar o tráfego para vários recursos nas proporções que você especificar. Você pode usar roteamento ponderado para criar registros em uma zona hospedada privada.

Tópicos

- Roteamento ponderado
- Como o Amazon Route 53 usa o EDNS0 para estimar a localização de um usuário

Roteamento simples

O roteamento simples permite configurar registros de DNS padrão sem roteamento especial do Route 53, como ponderados ou de latência. Com o roteamento simples, você normalmente roteia o tráfego para um único recurso, por exemplo, para um servidor web do seu site.

Você pode usar uma política de roteamento simples para criar registros em uma zona hospedada privada.

Se você escolher a política de roteamento simples no console do Route 53, não poderá criar vários registros com o mesmo nome e tipo, mas poderá especificar diversos valores no mesmo registro, como vários endereços IP. (Se você escolher a política de roteamento simples para um registro de alias, poderá especificar somente um AWS recurso ou um registro na zona hospedada atual.) Se você especificar diversos valores em um registro, o Route 53 retornará todos os valores para o resolvedor recursivo em ordem aleatória, e o resolvedor retornará os valores para o cliente (como um navegador da Web) que enviou a consulta de DNS. Em seguida, o cliente escolhe um valor e reenvia a consulta. Com uma política de roteamento simples, embora você possa especificar vários endereços IP, esses endereços IP não têm a integridade verificada.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento simples para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros simples
- Valores específicos para registros de alias simples
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Roteamento de failover

O roteamento de failover permite rotear o tráfego para um recurso quando o recurso estiver íntegro ou para um recurso diferente quando o primeiro recurso não estiver íntegro. Os registros primários e secundários podem encaminhar o tráfego para qualquer ponto a partir de um bucket do Amazon S3 que é configurado como um site para uma árvore complexa de registros. Para ter mais informações, consulte Failover ativo/passivo.

Você pode usar uma política de roteamento por failover para criar registros em uma zona hospedada privada.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento de failover para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros de failover
- Valores específicos para registros de alias de failover
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Roteamento de localização geográfica

O roteamento de localização geográfica permite que você escolha os recursos que atendem ao seu tráfego com base na localização geográfica dos usuários, isto é, o local de origem das consultas de DNS. Por exemplo, talvez você queira que todas as consultas da Europa sejam roteadas para um balanceador de carga de Elastic Load Balancing na região de Frankfurt.

Quando você usa o roteamento de localização geográfica, pode traduzir o conteúdo e apresentar todo o seu site ou parte dele no idioma de seus usuários. Você também pode usar o roteamento de localização geográfica para restringir a distribuição de conteúdo somente aos locais em que você tem direitos de distribuição. Outro uso possível é balancear a carga entre os endpoints de forma previsível, de easy-to-manage forma que a localização de cada usuário seja roteada de forma consistente para o mesmo endpoint.

Você pode especificar localizações geográficas por continente, país ou estado nos Estados Unidos. Se você criar registros separados para regiões geográficas sobrepostas, por exemplo, um registro para a América do Norte e outro para o Canadá, a prioridade será da menor região geográfica. Isso permite rotear algumas consultas de um continente para um recurso e rotear as consultas de determinados países naquele continente para outro recurso. (Para obter uma lista dos países de cada continente, consulte Local.)

A localização geográfica funciona através do mapeamento de endereços IP para os locais. No entanto, alguns endereços IP não estão mapeados para localizações geográficas. Portanto, mesmo que você crie conjuntos de registros de recursos de localização geográfica que abranja os sete continentes, o Amazon Route 53 receberá algumas consultas de DNS de locais que ele não conseguirá identificar. Você pode criar um registro padrão que atenda tanto as consultas de endereços IP que não são mapeados para qualquer lugar quanto as consultas que vêm de locais

para os quais você ainda não criou registros de localização geográfica. Se você não criar um registro padrão, o Route 53 retornará uma resposta “sem resposta” para as consultas provenientes desses locais.

Você pode usar o roteamento por geolocalização para criar registros tanto em uma zona hospedada privada como pública.

Para ter mais informações, consulte Como o Amazon Route 53 usa o EDNS0 para estimar a localização de um usuário.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento de geolocalização para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros de localização geográfica
- Valores específicos para registros de alias de localização geográfica
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Roteamento de geolocalização em zonas hospedadas privadas

Para zonas hospedadas privadas, o Route 53 responde às consultas de DNS com base na VPC da qual Região da AWS a consulta se originou. Para ver a lista de Regiões da AWS, consulte Regiões e zonas no guia do usuário do Amazon EC2.

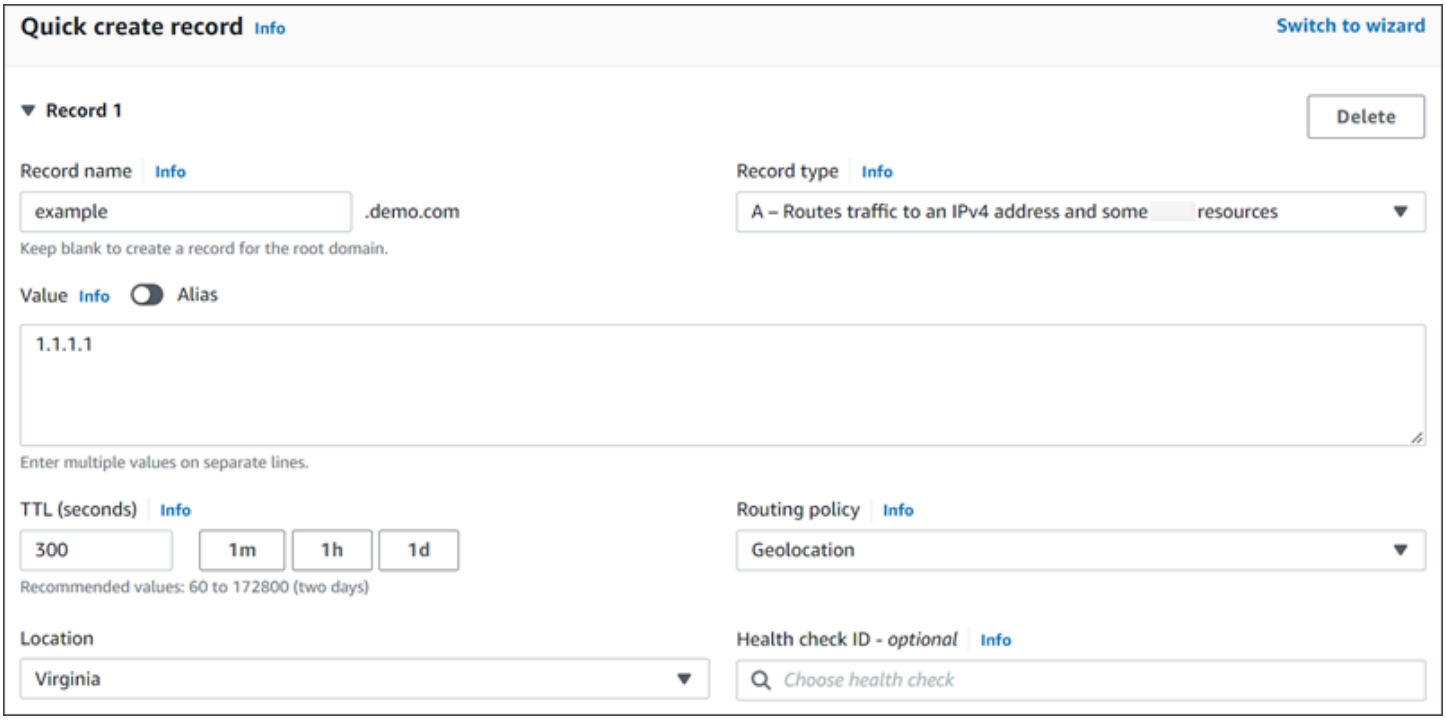
Se a consulta ao DNS for originada de uma parte on-premises de uma rede híbrida, ela será considerada como tendo sido originada da Região da AWS em que a VPC está localizada.

Se você incluir verificações de integridade, poderá criar registros padrão para:

- Endereços IP que não são mapeados para localizações geográficas.
- Consultas ao DNS provenientes de locais para os quais você não criou registros de geolocalização.

Se o registro de geolocalização para a região da consulta ao DNS não estiver íntegro, o registro padrão será retornado (se estiver íntegro).

No exemplo de configuração na figura a seguir, as consultas de DNS provenientes de um us-east-1 Região da AWS (Virgínia) serão roteadas para o endpoint 1.1.1.1.



Roteamento por geoproximidade

O roteamento de proximidade geográfica permite que o Amazon Route 53 encaminhe o tráfego para seus recursos com base no local geográfico de seus usuários e recursos. Ele direciona o tráfego para o recurso mais próximo disponível. Você também pode optar por rotear mais ou menos tráfego para um determinado recurso especificando um valor, conhecido como desvio. Um desvio aumenta ou diminui o tamanho da região geográfica em que o tráfego é roteado para um recurso.

Você cria regras de geoproximity para seus recursos e especifica um dos seguintes valores para cada regra:

- Se você estiver usando AWS recursos, especifique o Região da AWS ou o Grupo de Zona Local no qual você criou o recurso.
- Se você não estiver usando AWS recursos, especifique a latitude e a longitude do recurso.

Para usar as Zonas AWS Locais, você precisa primeiro habilitá-las. Para mais informações, consulte Getting started with Local Zones no AWS Local Zones User Guide.

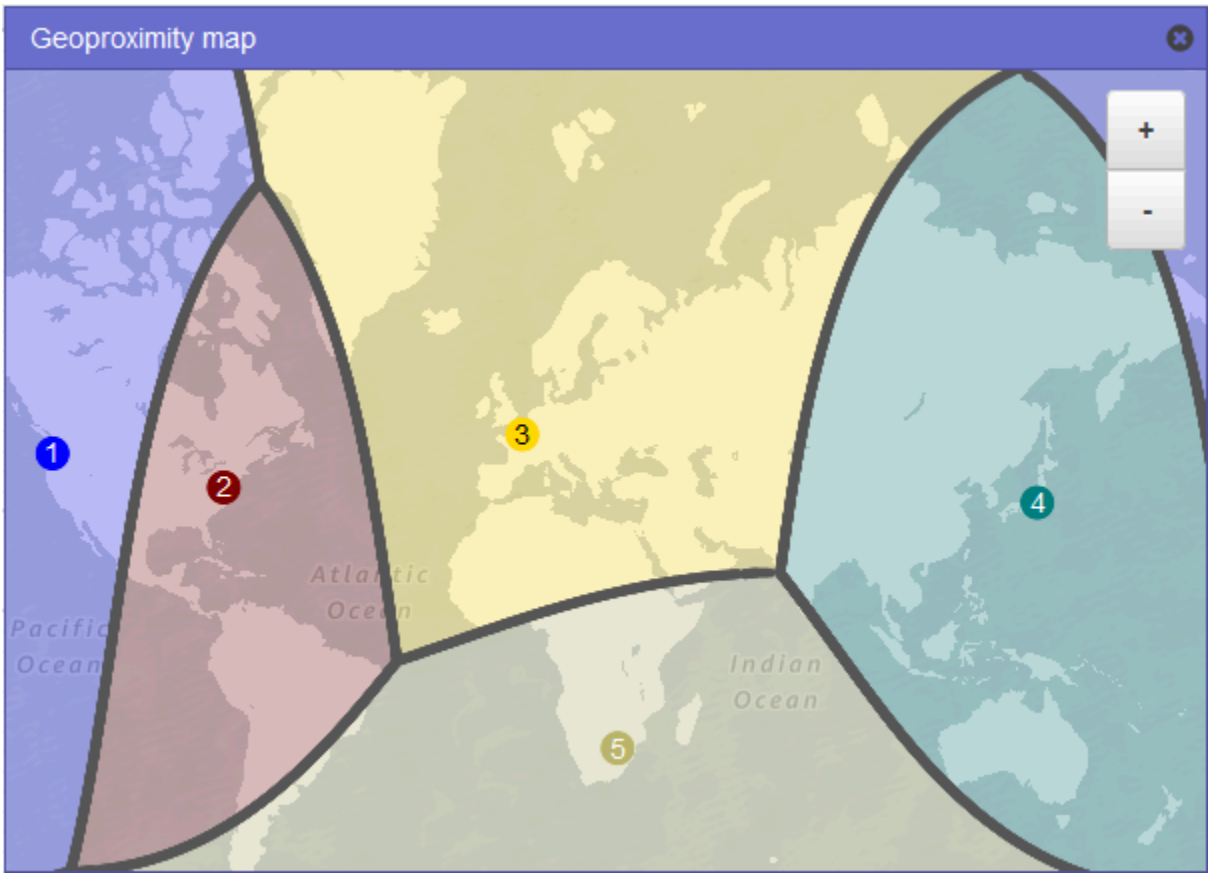
Para saber mais sobre a diferença entre Zonas Locais Regiões da AWS e Zonas Locais, consulte Regiões e Zonas no Guia do Usuário do Amazon EC2.

Opcionalmente, para alterar o tamanho da região geográfica da qual o Route 53 encaminha o tráfego para um recurso, especifique o valor aplicável para o desvio:

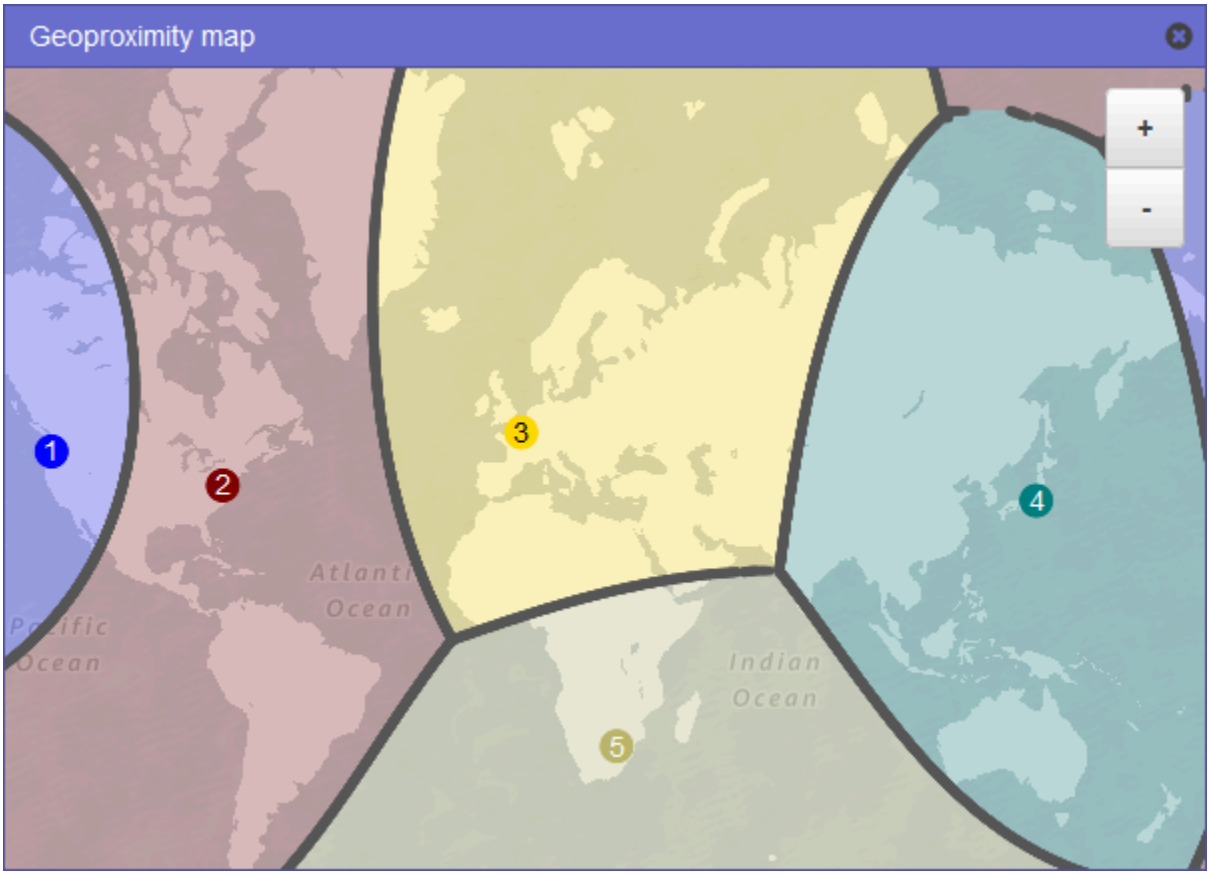
- Para aumentar o tamanho da região geográfica da qual o Route 53 encaminha o tráfego para um recurso, especifique um inteiro positivo de 1 a 99 para o desvio. O Route 53 diminui o tamanho das regiões adjacentes.
- Para reduzir o tamanho da região geográfica da qual o Route 53 encaminham o tráfego para um recurso, especifique um inteiro negativo de -1 a -99 para o desvio. O Route 53 aumenta o tamanho das regiões adjacentes.

O mapa a seguir mostra quatro Regiões da AWS (numerados de 1 a 4) e uma localização em Joanesburgo, África do Sul, especificada por latitude e longitude (5).

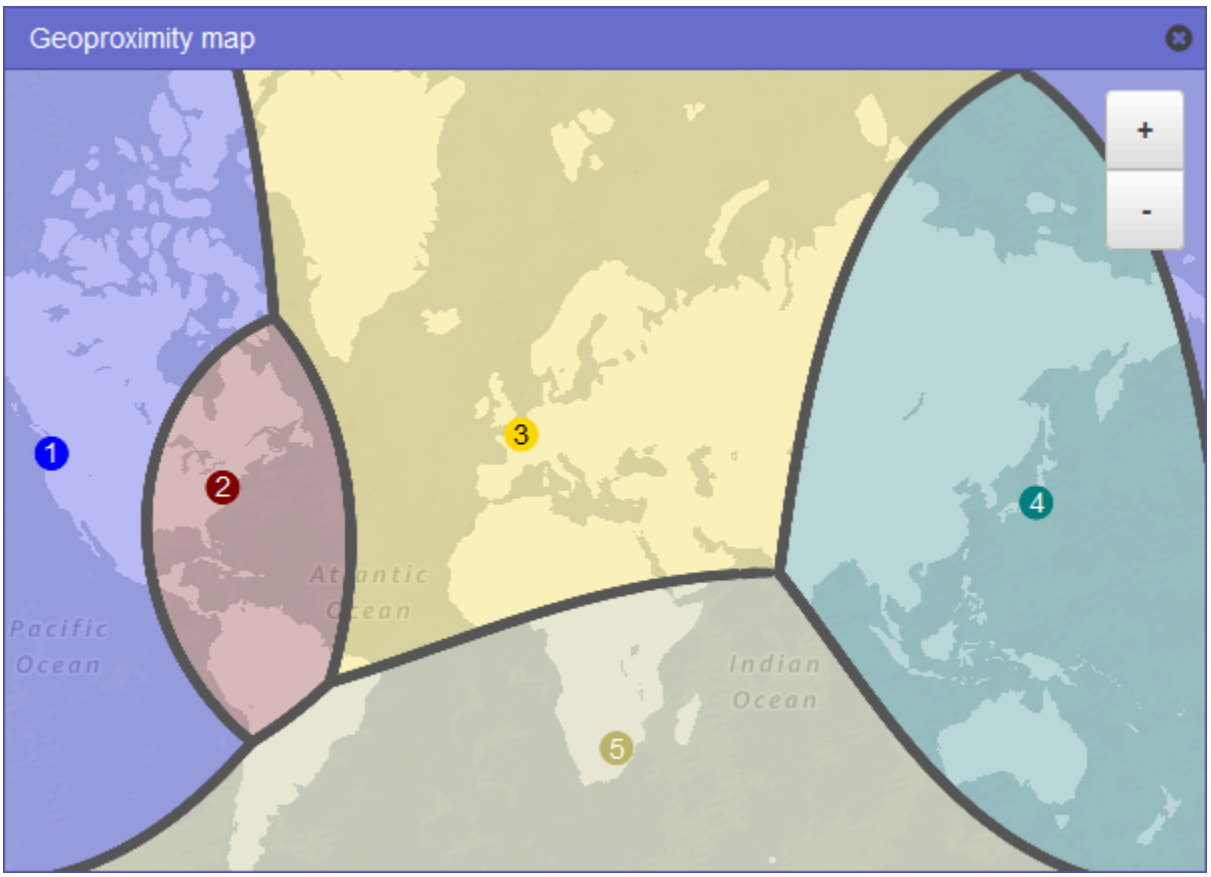
> **Note**
>
> Os mapas estão disponíveis somente com o fluxo de tráfego.



O mapa a seguir mostra o que acontece se você adicionar um desvio de +25 para a região Leste dos EUA (N. da Virgínia) (número 2 no mapa). O tráfego é roteado para o recurso nessa região de uma parte maior da América do Norte que anteriormente, e de toda a América do Sul.



O mapa a seguir mostra o que acontece se você alterar o desvio para -25 para a região Leste dos EUA (N. da Virgínia). O tráfego é roteado para o recurso nessa região de partes menores da América do Norte e do Sul do que anteriormente, e mais tráfego é roteado para os recursos nas regiões adjacentes 1, 3, e 5.



O efeito da alteração do desvio para seus recursos depende de uma série de fatores, incluindo:

- O número de recursos que você tem.
- A proximidade de um para outro.
- O número de usuários que você tem perto da área de borda entre as regiões geográficas. Por exemplo, suponha que você tenha recursos no Leste dos Regiões da AWS EUA (Norte da Virgínia) e no Oeste dos EUA (Oregon) e tenha muitos usuários em Dallas, Austin e San Antonio, Texas, EUA. Essas cidades são aproximadamente equidistantes entre seus recursos, portanto, uma pequena mudança no viés pode resultar em uma grande variação no tráfego de recursos de uma Região da AWS para outra.

Recomendamos alterar o desvio em pequenos incrementos para evitar a sobrecarga dos recursos devido a uma oscilação imprevista no tráfego.

Para ter mais informações, consulte Como o Amazon Route 53 usa o EDNS0 para estimar a localização de um usuário.

Como o Amazon Route 53 usa o desvio para encaminhar o tráfego

Esta é a fórmula que o Amazon Route 53 usa para determinar como encaminhar o tráfego:

Viés

```
Biased distance = actual distance * [1 - (bias/100)]
```

Quando o valor do viés é positivo, o Route 53 trata a origem de uma consulta de DNS e o recurso que você especifica em um registro de geoproximidade (como uma instância do EC2 em um Região da AWS) como se estivessem mais próximos do que realmente estão. Por exemplo, suponha que você tem uma solicitação com os seguintes registros de geoproximity:

- Um registro para o servidor web A, que tem um desvio positivo de 50
- Um registro para o servidor web B, que não tem desvio

Quando um registro de proximidade geográfica tem um desvio positivo de 50, o Route 53 divide a distância pela metade entre a origem de uma consulta e o recurso para esse registro. Em seguida, o Route 53 calcula qual recurso está mais próximo da origem da consulta. Suponha que o servidor web A está a 150 km da origem de uma consulta e o servidor web B está a 100 km da origem da consulta. Se nenhum dos registros tiver um desvio, o Route 53 encaminha a consulta para o servidor Web B, pois ele é o mais próximo. No entanto, como o registro do servidor Web A tem um desvio positivo de 50, o Route 53 trata o servidor Web A como se ele estivesse a 75 km da origem da consulta. Como resultado, o Route 53 encaminha a consulta para o servidor Web A.

Este é o cálculo para um desvio positivo de 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
```

Roteamento baseado em latência

Se seu aplicativo estiver hospedado em vários Regiões da AWS, você pode melhorar o desempenho de seus usuários atendendo às solicitações a partir do Região da AWS que fornece a menor latência.

> **Note**
>
> Os dados sobre a latência entre usuários e seus recursos são baseados totalmente no tráfego entre usuários e datacenters da AWS . Se você não estiver usando recursos em um Região da AWS, a latência real entre seus usuários e seus recursos pode variar significativamente dos dados de AWS latência. Isso ocorre mesmo se os recursos estiverem na mesma cidade que uma Região da AWS.

Para usar o roteamento baseado em latência, crie registros de latência para os recursos em várias Regiões da AWS. Quando o Route 53 recebe uma consulta ao DNS do seu domínio ou subdomínio (exemplo.com ou acme.exemplo.com), ele determina para quais Regiões da AWS você criou registros de latência, determina qual região oferece ao usuário a menor latência e então seleciona um registro de latência para essa região. O Route 53 responde com o valor do registro selecionado, como o endereço IP de um servidor Web.

Por exemplo, suponha que você tenha balanceadores de carga de Elastic Load Balancing na região Oeste dos EUA (Oregon) e na região Ásia-Pacífico (Singapura). Você cria um registro de latência para cada balanceador de carga. Veja o que acontece quando um usuário em Londres informa o nome de seu domínio em um navegador:

1. O DNS encaminha a consulta para um servidor de nome do Route 53.
2. O Route 53 consulta seus dados sobre latência entre Londres e a região de Singapura e entre Londres e a região de Oregon.
3. Se a latência for menor entre as regiões de Londres e Oregon, o Route 53 responderá à consulta com o endereço IP do balanceador de carga de Oregon. Se a latência for menor entre Londres e a região de Singapura, o Route 53 responderá com o endereço IP do balanceador de carga de Singapura.

A latência entre os hosts na Internet pode mudar com o tempo como resultado de alterações na conectividade de rede e no roteamento. O roteamento baseado em latência se baseia em medições de latência realizadas durante um período de tempo, e as medições refletem essas alterações. Uma solicitação roteada para a região de Oregon esta semana pode ser roteada para a região de Singapura a semana que vem.

> **Note**
>
> Quando um navegador ou outro visualizador usa um resolvedor de DNS compatível com a edns-client-subnet extensão EDNS0, o resolvedor de DNS envia ao Route 53 uma versão truncada do endereço IP do usuário. Se você configurar o encaminhamento por latência, o Route 53 considerará esse valor ao encaminhar o tráfego para seus recursos. Para ter mais informações, consulte Como o Amazon Route 53 usa o EDNS0 para estimar a localização de um usuário.

Você pode usar uma política de roteamento por latência para criar registros em uma zona hospedada privada.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento de latência para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros de latência
- Valores específicos para registros de alias de latência
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

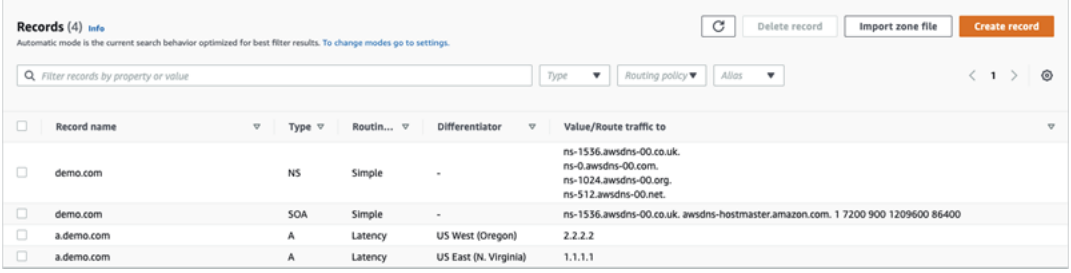
Roteamento baseado em latência em zonas hospedadas privadas

Para zonas hospedadas privadas, o Route 53 responde às consultas de DNS com um endpoint que está no mesmo Região da AWS ponto ou está mais próximo da VPC da qual Região da AWS a consulta se originou.

> **Note**
>
> Se você tiver um endpoint de saída encaminhado para um endpoint de entrada, o registro será resolvido com base na localização do endpoint de entrada, não do endpoint de saída.

Se você incluir verificações de integridade e o registro com a menor latência para a origem da consulta não estiver íntegro, um endpoint íntegro com a próxima latência mais baixa será retornado.

No exemplo de configuração na figura a seguir, as consultas de DNS provenientes de um us-east-1 Região da AWS, ou mais próximo a ele, serão roteadas para o endpoint 1.1.1.1. As consultas ao DNS de us-west-2, ou da região mais próxima a ela, serão roteadas para o endpoint 2.2.2.2.



Roteamento baseado em IP

Com o roteamento baseado em IP no Amazon Route 53, você pode ajustar o roteamento DNS usando a compreensão que tem da rede, das aplicações e dos clientes para tomar as melhores decisões de roteamento DNS para os usuários finais. O roteamento baseado em IP dá a você controle granular para otimizar a performance ou reduzir os custos de rede, carregando os dados no Route 53 na forma de mapeamentos de IP do usuário para endpoint.

O roteamento por geolocalização e o roteamento baseado em latência são baseados em dados que o Route 53 coleta e mantém atualizados. Essa abordagem funciona bem para a maioria dos clientes, mas o roteamento baseado em IP oferece a capacidade adicional de otimizar o roteamento com base no conhecimento específico da base de clientes. Por exemplo, um provedor global de conteúdo de vídeo talvez queira rotear os usuários finais de um determinado provedor de serviços de Internet (ISP).

Estes são alguns casos comuns de uso de roteamento baseado em IP:

- Você deseja rotear usuários finais de determinados ISPs para endpoints específicos a fim de otimizar os custos ou a performance do trânsito da rede.
- Você quer adicionar substituições aos tipos existentes de roteamento do Route 53, como roteamento por geolocalização, com base em seu conhecimento das localizações físicas dos clientes.

Gerenciar intervalos IP e associá-los a um conjunto de registros de recursos (RRSet)

Para IPv4, você pode usar blocos CIDR de 1 a 24 bits, enquanto para IPv6 você pode usar blocos CIDR de 1 a 48 bits. Para definir um bloco CIDR de zero bit (0.0.0.0/0 ou ::/0), use o local padrão ("*").

Para consultas ao DNS com um CIDR maior que o especificado na coleção CIDR, o Route 53 fará a correspondência com o CIDR mais curto. Por exemplo, se você especificar 2001:0DB8::/32 como o bloco CIDR em sua coleção CIDR e uma consulta se originar em 2001:0DB8:0000:1234::/48, ela encontrará uma correspondência. Se, por outro lado, você especificar 2001:0DB8:0000:1234::/48 em sua coleção CIDR e uma consulta se originar de 2001:0DB8::/32, não haverá correspondência e o Route 53 responderá com o registro do local padrão ("*").

Você pode agrupar conjuntos de blocos CIDR (ou intervalos IP) em locais CIDR, que, por sua vez, são agrupados em entidades reutilizáveis chamadas coleções CIDR:

CIDR block (Bloco CIDR)

Um intervalo IP na notação CIDR, por exemplo, 192.0.2.0/24 ou 2001: DB8:: /32.

Local CIDR

Uma lista nomeada de blocos CIDR. Por exemplo, example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:DB8: :/32]. Os blocos em uma lista de locais CIDR não precisam ser adjacentes ou o mesmo intervalo.

Um único local pode ter blocos IPv4 e IPv6, e pode estar associado tanto a conjuntos de registros A quanto AAAA, respectivamente.

O nome do local geralmente é um local, por convenção, mas pode ser qualquer string, por exemplo Empresa-A.

Coleção CIDR

Uma coleção nomeada de locais. Por exemplo, mycollection = [example-isp-seattle, example-isp-tokyo].

Os conjuntos de registros de recursos de roteamento baseados em IP referenciam um local em uma coleção, e todos os conjuntos de registros de recursos para o mesmo nome e tipo de conjunto de registros devem referenciar a mesma coleção. Por exemplo, se você criar sites em duas regiões e quiser direcionar consultas ao DNS de dois locais CIDR diferentes para um determinado site com base nos endereços IP de origem, ambos os locais devem estar listados na mesma coleção CIDR.

Você também pode compartilhar essas coleções entre AWS contas usando AWS RAM. Quando você faz uma atualização, como editar um dos intervalos IP em uma coleção, essa atualização é aplicada automaticamente a todos os conjuntos de registros associados à coleção.

Você não pode usar uma política de roteamento baseado em IP para criar registros em uma zona hospedada privada.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento simples para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros baseados em IP
- Valores específicos para registros de alias baseado em IP
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Tópicos

- Criar uma coleção CIDR com locais e blocos CIDR
- Trabalhar com locais e blocos CIDR
- Excluir uma coleção CIDR
- Mudar geolocalização para roteamento baseado em IP

Criar uma coleção CIDR com locais e blocos CIDR

Para começar, crie uma coleção CIDR e adicione a ela blocos e locais CIDR.

Para criar uma coleção CIDR usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione IP-based routing, (Roteamento baseado em IP) e depois CIDR collections. (Coleções CIDR).
3. Selecione Create CIDR collection (Criar coleção CIDR).
4. No painel Create CIDR collection (Criar coleção CIDR), em Details (Detalhes), insira um nome para a coleção.
5. Selecione Create collection (Criar coleção) para criar uma coleção vazia.

   - ou -

Na seção Create CIDR locations, insira um nome para o local do CIDR na caixa CIDR location. O nome do local pode ser qualquer string de identificação, por exemplo **`company 1`** ou **`Seattle`**. Não é necessário que seja um local geográfico real.

> **Important**
>
> O local do CIDR pode ter no máximo 16 caracteres.

Insira os blocos de CIDR na caixa CIDR blocks, um em cada linha. Estes endereços podem ser endereços IPv4 ou IPv6, indo de /0 a /24 para IPv4 e de /0 a /48 para IPv6.

6. Depois de inserir os blocos CIDR, selecione Create CIDR collection (Criar coleção CIDR) ou Add another location (Adicionar outro local) para continuar inserindo locais e blocos CIDR. Você pode inserir vários locais CIDR por coleção.
7. Após inserir os locais CIDR, selecione Create CIDR collection (Criar coleção CIDR).

Trabalhar com locais e blocos CIDR

Para trabalhar com locais CIDR usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione IP-based routing (Roteamento baseado em IP), CIDR collections (Coleções CIDR) e, na seção CIDR collections (Coleções CIDR), clique em um link para uma coleção CIDR da lista Collection name (Nome da coleção).

   Na página CIDR locations (Locais CIDR), você pode criar um local CIDR, excluí-lo ou editar um local e seus blocos.

   - Para criar um local, escolha Create CIDR location (Criar local CIDR).
   - No painel Create CIDR location (Criar local CIDR), insira um nome para o local, os blocos CIDR associados ao local e, depois, escolha Create (Criar).
   - Para exibir um local CIDR e os blocos do local, escolha o botão de opção ao lado de um local para exibir o nome e os blocos CIDR do local no painel de locais.

Neste painel, você também pode escolher Editar para atualizar o nome e/ou os blocos CIDR do local. Quando concluir a edição, escolha Save (Salvar).

- Para excluir um local CIDR e os blocos do local, escolha o botão ao lado do local que você deseja excluir e depois escolha Delete (Excluir). Para confirmar a exclusão, insira o nome do local no campo de entrada de texto e selecione Delete (Excluir) novamente.

> **Important**
>
> A exclusão de um local CIDR não pode ser desfeita. Se você tiver algum registro DNS associado ao local, seu domínio poderá ficar inacessível.

Excluir uma coleção CIDR

Para excluir uma coleção CIDR, os locais e blocos da coleção usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione IP-based routing, (Roteamento baseado em IP) e depois CIDR collections (Coleções CIDR).
3. Na seção CIDR collections (Coleções CIDR), clique no nome vinculado da coleção que você deseja excluir.
4. Na página CIDR locations (Locais CIDR), selecione um local de cada vez, escolha Delete (Excluir), insira o nome do local na caixa de diálogo e selecione Delete (Excluir). Você deve excluir todos os locais associados a uma coleção CIDR para poder excluí-la.
5. Após concluída a exclusão de todos os locais CIDR, na página CIDR locations (Locais CIDR), escolha o botão de opção ao lado da coleção que você deseja excluir e escolha Delete (Excluir).

Mudar geolocalização para roteamento baseado em IP

Se você estiver usando políticas de roteamento por geolocalização ou geoproximidade, e perceber que clientes específicos são consistentemente roteados para um endpoint que não é o ideal com base na localização física ou na topologia da rede, você pode direcionar melhor os intervalos de IP públicos desses clientes usando roteamento baseado em IP.

A tabela a seguir contém um exemplo de configuração de geolocalização para um roteamento por geolocalização existente que ajustaremos para intervalos de IP da Califórnia.

Nome do conjunto de registros	Política de roteamento e origem	Endereço IP do endpoint da aplicação
exemplo.com	Roteamento por localização geográfica (EUA)	`198.51.100.1`
exemplo.com	Roteamento por geolocalização (UE)	`198.51.100.2`

Para substituir intervalos de IP da Califórnia para ir para um novo endpoint de aplicação, primeiro, recrie o roteamento por geolocalização com um novo nome de conjunto de registros.

Nome do conjunto de registros	Política de roteamento e origem	Endereço IP do endpoint da aplicação
geo.example.com	Roteamento por localização geográfica (EUA)	`198.51.100.1`
geo.example.com	Roteamento por localização geográfica (EU)	`198.51.100.2`

Depois, crie registros de roteamento baseados em IP e um registro padrão que aponte para o conjunto recém-recriado de registros de roteamento por geolocalização.

Nome do conjunto de registros	Política de roteamento e origem	Endereço IP do endpoint da aplicação
exemplo.com	Roteamento baseado em IP (padrão)	Registro de alias para o endpoint da aplicação geo.exemplo.com que você

Nome do conjunto de registros	Política de roteamento e origem	Endereço IP do endpoint da aplicação
		deseja que seja o padrão. Por exemplo, `198.51.100.1` .
exemplo.com	Roteamento baseado em IP (intervalos de IP da Califórnia)	`198.51.100.3`

Roteamento de resposta com vários valores

O roteamento de resposta com valores múltiplos permite que você configure o Amazon Route 53 para retornar vários valores, como endereços IP de seus servidores Web, em resposta às consultas de DNS. Você pode especificar vários valores para praticamente qualquer registro, mas o roteamento de resposta com valores múltiplos também permite que você verifique a integridade de cada recurso de modo que o Route 53 retorna somente valores para recursos íntegros. Este tipo de roteamento não substitui o load balancer. No entanto, a capacidade de retornar vários endereços IP cuja integridade pode ser verificada é uma forma de usar o DNS para aprimorar a disponibilidade e o balanceamento de carga.

Para encaminhar o tráfego de forma aproximada e aleatória para vários recursos, como servidores Web, crie um registro de resposta de múltiplos valores para cada recurso e, se desejar, associe uma verificação de integridade do Route 53 a cada registro. O Route 53 responde às consultas de DNS com até oito registros íntegros e oferece respostas diferentes para resolvedores de DNS diferentes. Se um servidor web se tornar indisponível depois que um resolvedor armazenar uma resposta em cache, o software cliente pode tentar outro endereço IP na resposta.

Observe o seguinte:

- Se você associar uma verificação de integridade ao registro de resposta de múltiplos valores, o Route 53 responderá às consultas de DNS com o endereço IP correspondente apenas quando a verificação de integridade for íntegra.
- Se você não associar uma verificação de integridade a um registro de resposta de múltiplos valores, o Route 53 sempre considerará o registro como íntegro.
- Se você tiver oito ou menos registros íntegros, o Route 53 responderá a todas as consultas de DNS com todos os registros íntegros.

- Quando nenhum dos registros estiver íntegro, o Route 53 responderá às consultas DNS com até oito registros não íntegros.

Você pode usar roteamento por resposta com vários valores para criar registros em uma zona hospedada privada.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento de resposta de vários valores para criar registros, consulte Valores específicos para registros de resposta com valores múltiplos e Valores que são comuns para todas as políticas de roteamento.

Roteamento ponderado

O roteamento ponderado permite que você associe vários recursos a um único nome de domínio (exemplo.com) ou subdomínio (acme.exemplo.com) e escolha a quantidade de tráfego roteado para cada recurso. Isso pode ser útil para diversas finalidades, incluindo balanceamento de carga e teste de novas versões de software.

Para configurar o roteamento ponderado, crie registros que têm o mesmo nome e tipo de cada um dos seus recursos. A cada registro você atribui um peso relativo que corresponde à quantidade de tráfego que deseja enviar a cada recurso. O Amazon Route 53 envia o tráfego para um recurso com base no peso que você atribui ao registro como uma proporção do peso total para todos os registros no grupo:

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

Por exemplo, se você deseja enviar uma pequena parte do seu tráfego para um recurso e o restante para outro recurso, pode especificar pesos 1 e 255. O recurso com peso 1 recebe 1/256 do tráfego (1/[1+255]) e o outro recurso recebe 255/256 (255/[1+255]). Você pode alterar gradualmente o equilíbrio alterando os pesos. Se você deseja interromper o envio de tráfego para um recurso, pode alterar o peso desse registro para 0.

Para obter informações sobre os valores que você especifica ao usar a política de roteamento ponderada para criar registros, consulte os seguintes tópicos:

- Valores específicos para registros ponderados
- Valores específicos para registros de alias ponderados
- Valores que são comuns para todas as políticas de roteamento
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Você pode usar uma política de roteamento ponderado para criar registros em uma zona hospedada privada.

Verificações de integridade e roteamento ponderado

Se você adicionar verificações de integridade a todos os registros em um grupo de registros ponderados, mas atribuir pesos diferentes de zero a alguns registros e pesos iguais a zero a outros, as verificações de integridade funcionarão da mesma maneira que todos os registros com pesos diferentes de zero com as seguintes exceções:

- Inicialmente, o Route 53 considera somente os registros ponderados com valores diferentes de zero, se houver.
- Se nenhum dos registros com ponderação maior que zero estiver íntegro, o Route 53 considerará os registros com ponderação igual a zero.

A tabela a seguir detalha o comportamento quando o registro de peso 0 inclui uma verificação de integridade:

	Registro 1	Registro 2	Registro 3
Weight	1	1	0
Inclui verificação de integridade?	Sim	Sim	Sim
Status da verificação de integridade	Não integro	Não integro	Integridade
Consulta ao DNS respondida?	Não	Não	Sim
Status da verificação de integridade	Não integro	Não integro	Não integro

	Registro 1	Registro 2	Registro 3
Consulta ao DNS respondida?	Sim	Sim	Não
Status da verificação de integridade	Não integro	Integridade	Não integro
Consulta ao DNS respondida?	Não	Sim	Não
Status da verificação de integridade	Integridade	Integridade	Não integro
Consulta ao DNS respondida?	Sim	Sim	Não
Status da verificação de integridade	Integridade	Integridade	Integridade
Consulta ao DNS respondida?	Sim	Sim	Não

A tabela a seguir detalha o comportamento quando o registro de peso 0 não inclui uma verificação de integridade:

	Registro 1	Registro 2	Registro 3
Weight	1	1	0
	Sim	Sim	Não

	Registro 1	Registro 2	Registro 3
Inclui verificação de integridade?			
Status da verificação de integridade	Integridade	Integridade	N/D
Consulta ao DNS respondida?	Sim	Sim	Não
Status da verificação de integridade	Não integro	Não integro	N/D
Consulta ao DNS respondida?	Não	Não	Sim
Status da verificação de integridade	Não integro	Integridade	N/D
Consulta ao DNS respondida?	Não	Sim	Não

Como o Amazon Route 53 usa o EDNS0 para estimar a localização de um usuário

Para melhorar a precisão do roteamento por geolocalização, geoproximidade, baseado em IP e latência, o Amazon Route 53 suporta a extensão do EDNS0. edns-client-subnet (O EDNS0 adiciona várias extensões opcionais ao protocolo DNS.) O Route 53 pode ser usado edns-client-subnet somente quando os resolvedores de DNS o suportam:

- Quando um navegador ou outro visualizador usa um resolvedor de DNS que não oferece suporte edns-client-subnet, o Route 53 usa o endereço IP de origem do resolvedor de DNS para aproximar a localização do usuário e responde às consultas de geolocalização com o registro DNS da localização do resolvedor.

- Quando um navegador ou outro visualizador usa um resolvedor de DNS compatível edns-client-subnet, o resolvedor de DNS envia ao Route 53 uma versão truncada do endereço IP do usuário. O Route 53 determina o local do usuário com base no endereço IP truncado, em vez de usar o endereço IP de origem do resolvedor de DNS. Geralmente, isso fornece uma estimativa mais precisa do local do usuário. O Route 53 então responde às consultas de localização geográfica com o registro de DNS do local do usuário.
- O EDNS0 não é aplicável a zonas hospedadas privadas. Para zonas hospedadas privadas, o Route 53 usa dados dos resolvedores do Route 53 em Região da AWS que a zona hospedada privada está para tomar decisões de geolocalização e roteamento de latência.

Para obter mais informações sobre edns-client-subnet, consulte RFC da sub-rede do cliente EDNS, sub-rede do cliente em solicitações de DNS.

Escolher entre registros de alias e não alias

Os alias records (registros de alias) do Amazon Route 53 fornecem uma extensão específica do Route 53 para a funcionalidade do DNS. Os registros de aliases permitem que você direcione o tráfego para AWS recursos selecionados, incluindo, mas não se limitando a, CloudFront distribuições e buckets do Amazon S3. Eles também permitem rotear o tráfego de um registro em uma zona hospedada para outro registro.

Ao contrário do registro CNAME, você não pode criar um registro de alias no nó superior de um namespace DNS, também conhecido como o apex da zona. Por exemplo, se você registrar o nome do DNS exemplo.com, o apex de zona será exemplo.com. Você não pode criar um registro CNAME para exemplo.com, mas pode criar um registro de alias para exemplo.com que roteie o tráfego para www.exemplo.com (desde que o tipo de registro de www.exemplo.com não seja CNAME).

Quando o Route 53 recebe uma consulta de DNS para um registro de alias, o Route 53 responde com o valor aplicável para esse recurso:

- Uma API regional personalizada do Amazon API Gateway ou uma API otimizada para bordas: O Route 53 responde com um ou mais endereços IP para sua API.
- Um endpoint de interface da Amazon VPC: o Route 53 responde com um ou mais endereços IP para seu endpoint de interface.
- Uma CloudFront distribuição — o Route 53 responde com um ou mais endereços IP para servidores de CloudFront borda que podem servir seu conteúdo.

- Um ambiente do Elastic Beanstalk: o Route 53 responde com um ou mais endereços IP para o ambiente.
- Um balanceador de carga de Elastic Load Balancing: o Route 53 responde com um ou mais endereços IP para o balanceador de carga. Isso inclui Application Load Balancer, Classic Load Balancer e Network Load Balancer.
- Um AWS Global Accelerator acelerador — o Route 53 responde com os endereços IP do acelerador.
- Um bucket do Amazon S3 que é configurado como um site estático: o Route 53 responde a cada consulta com um endereço IP para o bucket do Amazon S3.
- Outro registro do Route 53 do mesmo tipo na mesma zona hospedada: o Route 53 responde como se a consulta fosse para o registro referenciado pelo registro de alias (consulte Comparação entre registros de alias e de CNAME).
- AWS AppSync nome de domínio — O Route 53 responde com um ou mais endereços IP para seu endpoint de interface.

Quando você usa um registro de alias para rotear o tráfego para um AWS recurso, o Route 53 reconhece automaticamente as alterações no recurso. Por exemplo, suponhamos que um registro de alias de exemplo.com aponte para um balanceador de carga de Elastic Load Balancing em lb1-1234.us-east-2.elb.amazonaws.com. Se o endereço IP do balanceador de carga for alterado, o Route 53 será iniciado automaticamente para responder a consultas DNS usando o novo endereço IP.

Se um registro de alias apontar para um AWS recurso, você não poderá definir o tempo de vida (TTL); o Route 53 usa o TTL padrão para o recurso. Se um registro de alias aponta para outro registro na mesma zona hospedada, o Route 53 usa o TTL do registro para o qual que o registro de alias aponta. Para obter mais informações sobre o valor de TTL atual do Elastic Load Balancing, acesse Request routing (Roteamento de solicitação) no Manual do usuário do Elastic Load Balancing e procure por “ttl”.

Para obter informações sobre como criar registros usando o console do Route 53, consulte Criar registros usando o console do Amazon Route 53. Para obter informações sobre os valores que você especifica para registros de alias, consulte o tópico aplicável em Valores que você especifica ao criar ou editar registros do Amazon Route 53:

- Valores específicos para registros de alias simples
- Valores específicos para registros de alias ponderados

- Valores específicos para registros de alias de latência
- Valores específicos para registros de alias de failover
- Valores específicos para registros de alias de localização geográfica
- Valores específicos para registros de alias de geoproximidade
- Valores que são comuns para registros de alias em todas as políticas de roteamento

Comparação entre registros de alias e de CNAME

Os registros de alias são semelhantes a registros CNAME, mas há algumas diferenças importantes. A lista a seguir compara registros de alias e registros CNAME.

Recursos para os quais é possível redirecionar consultas

Registros de alias

Um registro de alias só pode redirecionar consultas para AWS recursos selecionados, incluindo, mas não se limitando ao seguinte:

- Buckets do Amazon S3
- CloudFront distribuições
- Outro registro na mesma zona hospedada do Route 53

Por exemplo, você pode criar um registro de alias chamado acme.example.com que redireciona as consultas para um bucket do Amazon S3 que também é chamado de acme.example.com. Você também pode criar um registro de alias acme.example.com que redireciona as consultas para um registro chamado zenith.example.com na zona hospedada exemplo.com.

Registros CNAME

Um registro CNAME pode redirecionar consultas de DNS para qualquer registro de DNS. Por exemplo, você pode criar um registro CNAME que redireciona as consultas de acme.example.com para zenith.example.com ou para acme.example.org. Você não precisa usar o Route 53 como o serviço de DNS para o domínio ao qual está redirecionando consultas.

Criar registros com o mesmo nome do domínio (registros no apex de zona)

Registros de alias

Na maioria das configurações, você pode criar um registro de alias com o mesmo nome da zona hospedada (o apex de zona). A única exceção é quando você deseja redirecionar consultas de apex de zona (como example.com) para um registro na mesma zona hospedada com um tipo de CNAME (como zenith.example.com). O registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Registros CNAME

Não é possível criar um registro CNAME que tenha o mesmo nome da zona hospedada (a apex de zona). Isso é válido tanto para zonas hospedadas para nomes de domínio (exemplo.com) e para zonas hospedadas para subdomínios (zenith.example.com).

Definição de preço para consultas de DNS

Registros de alias

O Route 53 não cobra por consultas de alias aos AWS recursos. Para obter mais informações, consulte Definição de preço do Amazon Route 53.

Registros CNAME

O Route 53 cobra as consultas CNAME.

> **Note**
>
> Se você criar um registro CNAME que redireciona para o nome de outro registro em uma zona hospedada do Route 53 (a mesma zona hospedada ou outra zona hospedada), cada consulta de DNS será cobrada como duas consultas:
>
> - O Route 53 responde à primeira consulta de DNS com o nome do registro para o qual você deseja redirecionar.
> - Depois, o resolvedor de DNS deve enviar outra consulta para o registro na primeira resposta a fim de obter informações sobre o direcionamento do tráfego, por exemplo, o endereço IP de um servidor web.
>
> Se o registro CNAME for redirecionado para o nome de um registro hospedado com outro serviço de DNS, o Route 53 cobrará por uma consulta. O outro serviço de DNS pode cobrar pela segunda consulta.

Tipo de registro especificado na consulta de DNS

Registros de alias

O Route 53 responde a uma consulta de DNS apenas quando o nome do registro de alias (como acme.example.com) e o tipo do registro de alias (como A ou AAAA) corresponder ao nome e ao tipo na consulta de DNS.

Registros CNAME

Um registro CNAME redireciona consultas de DNS para um nome de registro, independentemente do tipo de registro especificado na consulta de DNS, como A ou AAAA.

Como os registros são listados em consultas dig ou nslookup

Registros de alias

Na resposta a uma consulta dig ou nslookup, um registro de alias é listado como o tipo de registro que você especificou ao criar o registro, como A ou AAAA. (O tipo de registro especificado para um registro de alias depende do recurso para o qual você está encaminhando o tráfego. Por exemplo, para encaminhar o tráfego para um bucket do S3, especifique A para o tipo.) A propriedade alias é visível somente no console do Route 53 ou na resposta a uma solicitação programática, como um comando da CLI AWS . `list-resource-record-sets`

Registros CNAME

Um registro CNAME é listado como um registro CNAME em resposta às consultas dig ou nslookup.

Tipos de registro de DNS com suporte

O Amazon Route 53 oferece suporte aos tipos de registros de DNS listados nesta seção. Cada tipo de registro também inclui um exemplo de como formatar o elemento `Value` ao acessar o Route 53 usando a API.

> **Note**
>
> Para os tipos de registros que incluem um nome de domínio, digite um nome de domínio totalmente qualificado, como www.exemplo.com. O ponto final é opcional; o Route 53 pressupõe que o nome do domínio seja totalmente qualificado. Isso significa que o Route

53 trata www.exemplo.com (sem um ponto final) e www.exemplo.com. (com um ponto final) como valores idênticos.

O Route 53 fornece uma extensão para a funcionalidade DNS conhecida como registros de alias. Semelhantes aos registros CNAME, os registros de alias permitem que você encaminhe o tráfego para recursos da AWS selecionados, como as distribuições do CloudFront e os buckets do Amazon S3. Para obter mais informações, incluindo uma comparação entre registros de alias e CNAME, consulte Escolher entre registros de alias e não alias.

Tópicos

Tipo de registro A

Use um registro A para rotear o tráfego para um recurso, como um servidor web, usando um endereço IPv4 em notação decimal com ponto.

Exemplo para o console do Amazon Route 53

```
192.0.2.1
```

Exemplo para a API do Route 53

```
<Value>192.0.2.1</Value>
```

Tipo de registro AAAA

Use um registro AAAA para rotear o tráfego para um recurso, como servidor web, usando um endereço IPv6 em formato hexadecimal separado por dois pontos.

Exemplo para o console do Amazon Route 53

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Exemplo para a API do Route 53

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

Tipo de registro CAA

Um registro CAA especifica quais autoridades de certificação (CAs) têm permissão para emitir certificados para um domínio ou subdomínio. A criação de um registro CAA ajuda a impedir que CAs incorretas emitam certificados para seus domínios. Um registro CAA não é um substituto para os requisitos de segurança que são especificados por sua autoridade de certificação, como o requisito para validar que você é o proprietário de um domínio.

Você pode usar registros CAA para especificar:

- Quais autoridades de certificação (CAs) podem emitir certificados SSL/TLS, se houver
- O endereço de e-mail ou o URL a ser contatado quando a CA emitir um certificado para o domínio ou o subdomínio

Quando você adiciona um registro CAA a sua zona hospedada, você especifica três configurações separadas por espaços:

```
flags tag "value"
```

Observe o seguinte sobre o formato dos registros CAA:

- O valor de `tag` pode conter somente os caracteres A-Z, a-z e 0-9.

- Sempre coloque o `value` entre aspas ("").
- Algumas CAs permitem ou exigem valores adicionais para `value`. Especifique valores adicionais como pares de nome e valor, e separe-os com ponto-e-vírgula (;), por exemplo:

  ```
  0 issue "ca.example.net; account=123456"
  ```
- Se um CA recebe uma solicitação de certificado para um subdomínio (como www.example.com) e se não existe nenhum registro CAA no subdomínio, o CA envia uma consulta de DNS para um registro CAA para o domínio pai (como example.com). Se existir um registro para o domínio pai e se a solicitação de certificado for válida, o CA emitirá o certificado para o subdomínio.
- Recomendamos que você consulte sua CA para determinar quais valores especificar para um registro da CAA.
- Não é possível criar um registro de CAA e um registro do CNAME com o mesmo nome, pois o DNS não permite usar o mesmo nome para um registro do CNAME e para qualquer outro tipo de registro ao mesmo tempo.

Tópicos

Autorizar um CA a emitir um certificado para um domínio ou subdomínio

Para autorizar um CA a emitir um certificado para um domínio ou subdomínio, crie um registro com o mesmo nome do domínio ou do subdomínio, e especifique as seguintes configurações:

- flags: `0`
- Tag: `issue`
- value: o código da CA que você autoriza para emitir um certificado para o domínio ou subdomínio

Por exemplo, suponha que você deseja autorizar ca.example.net a emitir um certificado para example.com. Você cria um registro CAA para example.com com as seguintes configurações:

```
0 issue "ca.example.net"
```

Para obter informações sobre como autorizar o AWS Certificate Manager a emitir um certificado, consulte Configurar um registro CAA no AWS Certificate Manager Manual do usuário.

Autorizar um CA a emitir um certificado curinga para um domínio ou subdomínio

Para autorizar um CA a emitir um certificado curinga para um domínio ou subdomínio, crie um registro com o mesmo nome de domínio ou subdomínio, e especifique as seguintes configurações. Um certificado curinga se aplica ao domínio ou subdomínio e a todos os seus subdomínios.

- flags: `0`
- Tag: `issuewild`
- value (valor): o código da CA que você autoriza para emitir um certificado para um domínio ou subdomínio e seus subdomínios

Por exemplo, suponha que você deseja autorizar ca.example.net a emitir um certificado curinga para example.com, aplicável a example.com e a todos os seus subdomínios. Você cria um registro CAA para example.com com as seguintes configurações:

```
0 issuewild "ca.example.net"
```

Quando você quiser autorizar um CA a emitir um certificado curinga para um domínio ou subdomínio, crie um registro com o mesmo nome do domínio ou subdomínio, e especifique as seguintes configurações. Um certificado curinga se aplica ao domínio ou subdomínio e a todos os seus subdomínios.

Impedir qualquer CA de emitir um certificado para um domínio ou subdomínio

Para impedir qualquer CA de emitir um certificado para um domínio ou subdomínio, crie um registro com o mesmo nome do domínio ou subdomínio, e especifique as seguintes configurações:

- flags: `0`
- Tag: `issue`
- value (valor): `";"`

Por exemplo, suponha que você deseja impedir que qualquer CA emita um certificado para example.com. Você cria um registro CAA para example.com com as seguintes configurações:

```
0 issue ";"
```

Se você deseja impedir que qualquer CA emita um certificado para example.com ou seus subdomínios, crie um registro CAA para example.com com as seguintes configurações:

```
0 issuewild ";"
```

> **Note**
>
> Se você criar um registro CAA para example.com e especificar os valores a seguir, um CA que esteja usando o valor ca.example.net poderá emitir o certificado para example.com:
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

Solicitar que um CA entre em contato com você caso receba uma solicitação de certificado inválida

Se você deseja que qualquer CA que receba uma solicitação inválida para um certificado entre em contato com você, especifique as seguintes configurações:

- flags: `0`
- Tag: `iodef`
- value (valor): a URL ou o endereço de e-mail que você deseja que a CA notifique quando receber uma solicitação inválida de um certificado. Use o formato aplicável:

  `"mailto:`*email-address*`"`

  `"http://`*URL*`"`

  `"https://`*URL*`"`

Por exemplo, se você deseja que qualquer CA que receba uma solicitação inválida para um certificado envie um e-mail para admin@example.com, crie um registro de CAA com as seguintes configurações:

```
0 iodef "mailto:admin@example.com"
```

Usar outra configuração que é compatível com o CA

Se o seu CA oferece suporte a um recurso que não está definido na RFC para registros de CAA, especifique as seguintes configurações:

- flags: 128 (esse valor impede que a CA emita um certificado, se ela não ela não oferecer suporte ao recurso especificado.)
- tag: a tag que você autoriza a CA a usar
- value: o valor que corresponde ao valor da tag

Por exemplo, suponha que o CA oferece suporte ao envio de uma mensagem de texto caso receba uma solicitação inválida para certificado. (Não estamos ciente de quaisquer CAs que ofereçam suporte a essa opção.) As configurações para o registro poderiam ser:

```
128 exampletag "15555551212"
```

Exemplos

Exemplo para o console do Route 53

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Exemplo para a API do Route 53

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

Tipo de registro CNAME

Um registro CNAME mapeia consultas DNS para o nome do registro atual, como acme.example.com, para outro domínio (example.com ou example.net) ou subdomínio (acme.example.com ou zenith.example.org).

> **Important**
>
> O protocolo DNS não permite que você crie um registro CNAME no nó superior de um namespace DNS, também conhecido como o apex de zona. Por exemplo, se você registrar o nome do DNS exemplo.com, o apex de zona será exemplo.com. Você não pode criar um registro CNAME para exemplo.com, mas pode criar registros CNAME para www.exemplo.com, produtonovo.exemplo.com e assim por diante.
> Além disso, se você criar um registro CNAME para um subdomínio, não poderá criar outros registros para esse subdomínio. Por exemplo, se você criar um CNAME para www.example.com, não poderá criar outros registros para os quais o valor do campo Name (Nome) é www.example.com.

O Amazon Route 53 também oferece suporte para registros com alias, que permitem encaminhar consultas para recursos selecionados da AWS, como distribuições do CloudFront e buckets do Amazon S3. Os aliases têm algumas semelhanças com o tipo de registro CNAME. No entanto, você pode criar um alias para o apex de zona. Para obter mais informações, consulte Escolher entre registros de alias e não alias.

Exemplo para o console do Route 53

```
hostname.example.com
```

Exemplo para a API do Route 53

```
<Value>hostname.example.com</Value>
```

Tipo de registro de DS

Um registro de signatário de delegação (DS) refere-se a uma chave de zona para uma zona de subdomínio delegado. Você pode criar um registro de DS ao estabelecer uma cadeia de confiança ao configurar a assinatura DNSSEC. Para obter mais informações sobre como configurar o DNSSEC no Route 53, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

Os três primeiros valores são números decimais que representam a tag de chave, o algoritmo e o tipo de resumo. O quarto valor é o resumo da chave de zona. Para obter mais informações sobre o formato de DS, consulte RFC 4034.

Exemplo para o console do Route 53

```
123 4 5 1234567890abcdef1234567890absdef
```

Exemplo para a API do Route 53

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

Tipo de registro MX

Um registro MX especifica os nomes dos servidores de e-mail e, se você tiver dois ou mais servidores de e-mail, a ordem de prioridade. Cada valor de um registro MX contém dois valores, prioridade e nome de domínio.

Priority

Um número inteiro que representa a prioridade para um servidor de e-mail. Se você especificar somente um servidor, a prioridade pode ser qualquer inteiro entre 0 e 65535. Se você especificar vários servidores, o valor especificado para a prioridade indica para qual servidor de e-mail você deseja que o e-mail seja roteado para em primeiro lugar, em segundo e assim por diante. O servidor com o menor valor para a prioridade tem precedência. Por exemplo, se você tiver dois servidores de e-mail e especificar valores de 10 e 20 para a prioridade, o e-mail sempre vai para o servidor com uma prioridade 10, a não ser que ele esteja indisponível. Se você especificar valores de 10 e 10, o e-mail será roteado para os dois servidores de forma praticamente igual.

Nome de domínio

O nome do domínio do servidor de e-mail. Especifique o nome (como email.exemplo.com) de um registro A ou AAAA. Em RFC 2181, Classificações para a especificação DNS, a seção 10.3 proíbe especificar o nome de um registro do CNAME para o valor do nome de domínio. (Quando a RFC menciona “alias”, significa um registro do CNAME, não um registro de alias do Route 53.)

Exemplo para o console do Amazon Route 53

```
10 mail.example.com
```

Exemplo para a API do Route 53

```
<Value>10 mail.example.com</Value>
```

Tipo de registro NAPTR

O Name Authority Pointer (NAPTR – Ponteiro de autoridade de nome) é um tipo de registro usado pelas aplicações Dynamic Delegation Discovery System (DDDS – Sistema de descoberta de delegação dinâmica) para converter um valor em outro ou substituir um valor por outro. Por exemplo, um uso comum é converter números de telefone em SIP URIs.

O elemento `Value` de um registro NAPTR consiste em seis valores separados por espaço:

Ordem

Quando você especifica mais de um registro, a sequência na qual deseja que a aplicação DDDS avalie os registros. Valores válidos: 0 - 65535.

Preferência

Quando você especifica dois ou mais registros que têm a mesma ordem, sua preferência para a sequência na qual os registros são avaliados. Por exemplo, se dois registros têm uma ordem de 1, a aplicação DDDS primeiro avalia o registro que tem a menor preferência. Valores válidos: 0 - 65535.

Sinalizadores

Uma configuração específica para as aplicações DDDS. Os valores atualmente definidos na RFC 3404 são letras maiúsculas e minúsculas "A", "P", "S"e "U"e a string vazia "". Coloque os sinalizadores entre aspas.

Serviço

Uma configuração específica para as aplicações DDDS. Coloque o serviço entre aspas.

Para obter mais informações, consulte as RFCs aplicáveis:

- Aplicação DDDS do URI: https://tools.ietf.org/html/rfc3404#section-4.4
- Aplicação DDDS de S-NAPTR: https://tools.ietf.org/html/rfc3958#section-6.5
- Aplicação DDDS de U-NAPTR: https://tools.ietf.org/html/rfc4848#section-4.5

Regexp

Uma expressão regular que a aplicação DDDS usa para converter um valor de entrada em um valor de saída. Por exemplo, um sistema de telefone IP pode usar uma expressão regular para converter um número de telefone inserido por um usuário em um SIP URI. Coloque Regexp entre aspas. Especifique um valor para Regexp ou um valor para Substituição, mas não para ambos.

A expressão regular pode incluir qualquer um dos seguintes caracteres ASCII imprimíveis:

- a-z
- 0-9
- - (hífen)
- (espaço)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- " (aspas). Para incluir uma citação literal em uma string, preceda-a de um caractere \: \".
- \ (barra invertida). Para incluir uma barra invertida em uma string, preceda-a de um caractere \: \\.

Especifique todos os outros valores, como nomes de domínio internacionalizados, no formato octal.

Para a sintaxe de Regexp, consulte RFC 3402, seção 3.2, Sintaxe de expressão de substituição

Substituição

O nome de domínio totalmente qualificado (FQDN) do próximo nome de domínio para o qual você deseja que a aplicação DDDS envie uma consulta de DNS. A aplicação DDDS substitui o valor de entrada pelo o valor que você especifica para Substituição, se houver. Especifique um valor para Regexp ou um valor para Substituição, mas não para ambos. Se você especificar um valor para Regexp, especifique um ponto (.) em Replacement (Substituição).

O nome do domínio pode incluir a-z, 0-9 e – (hífen).

Para obter mais informações sobre as aplicações DDDS e os registros NAPTR, consulte as seguintes RFCs:

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Exemplo para o console do 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!" .
```

Exemplo para a API do 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 de registro NS

Um registro de NS identifica os servidores de nome da zona hospedada. Observe o seguinte:

- O uso mais comum de um registro NS é controlar como o tráfego da Internet é roteado para um domínio. Para usar os registros em uma zona hospedada para rotear o tráfego para um domínio, atualize as configurações de registro de domínio para usar os quatro servidores de nomes no registro NS padrão. (Este é o registro NS que tem o mesmo nome que a zona hospedada.)
- É possível criar uma zona hospedada separada para um subdomínio (acme.example.com) e usar essa zona hospedada para rotear o tráfego de Internet para o subdomínio e seus subdomínios (subdomain.acme.example.com). Defina esta configuração, conhecida como “delegar a responsabilidade por um subdomínio a uma zona hospedada” ao criar outro registro NS na zona hospedada para o domínio raiz (example.com). Para obter mais informações, consulte Rotear tráfego para subdomínios.
- Os registros NS também são usados para configurar servidores de nomes de rótulo branco. Para obter mais informações, consulte Configurar servidores de nome de rótulo branco.

Para obter mais informações sobre registros de NS, consulte Registros de NS e SOA que o Amazon Route 53 cria para uma zona hospedada pública.

Exemplo para o console do Amazon Route 53

```
ns-1.example.com
```

Exemplo para a API do Route 53

```
<Value>ns-1.example.com</Value>
```

Tipo de registro PTR

Um registro PTR mapeia um endereço IP para o nome de domínio correspondente.

Exemplo para o console do Amazon Route 53

```
hostname.example.com
```

Exemplo para a API do Route 53

```
<Value>hostname.example.com</Value>
```

Tipo de registro SOA

Um registro de início de autoridade (SOA) fornece informações sobre um domínio e a zona hospedada correspondente do Amazon Route 53. Para obter informações sobre os campos em um registro de SOA, consulte Registros de NS e SOA que o Amazon Route 53 cria para uma zona hospedada pública.

Exemplo para o console do Route 53

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Exemplo para a API do Route 53

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

Tipo de registro SPF

Anteriormente, os registros de SPF eram usados para verificar a identidade do remetente de mensagens de e-mail. No entanto, não recomendamos mais que você crie registros cujo tipo de registro seja SPF. A RFC 7208, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, versão 1, foi atualizada para dizer "...sua existência e mecanismo definidos na [RFC4408] levaram a alguns problemas de interoperabilidade. Da mesma forma, seu uso não é mais apropriado para a SPF versão 1; as implementações não são para usá-la." Na RFC 7208, consulte a seção 14.1, The SPF DNS Record Type.

Em vez de um registro SPF, recomendamos que você crie um registro TXT que contém o valor aplicável. Para obter mais informações sobre os valores válidos, consulte o artigo da Wikipédia Sender Policy Framework.

Exemplo para o console do Amazon Route 53

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Exemplo para a API do Route 53

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Tipo de registro SRV

Um elemento `Value` de um registro SRV consiste em quatro valores separados por espaços. Os três primeiros valores são números decimais que representam prioridade, peso e porta. O quarto valor é um nome de domínio. Os registros de SRV são usados para acessar serviços, como um serviço para e-mail ou comunicações. Para obter informações sobre o formato de registros de SRV, consulte a documentação do serviço ao qual você deseja se conectar.

Exemplo para o console do Amazon Route 53

```
10 5 80 hostname.example.com
```

Exemplo para a API do Route 53

```
<Value>10 5 80 hostname.example.com</Value>
```

Tipo de registro TXT

Um registro TXT contém uma ou mais strings que estão entre aspas duplas (''). Quando você usar a política de roteamento simples, inclua todos os valores para um domínio (example.com) ou subdomínio (www.example.com) no mesmo registro TXT.

Tópicos

- Inserir valores de registro TXT
- Caracteres especiais em um valor de registro TXT
- Maiúsculas e minúsculas em um valor de registro TXT
- Exemplos

Inserir valores de registro TXT

Uma única string pode incluir até 255 caracteres, incluindo:

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

Se for necessário inserir um valor maior que 255 caracteres, quebre o valor em strings de 255 caracteres ou menos e coloque cada string entre aspas duplas ("). No console, liste todas as strings na mesma linha:

```
"String 1" "String 2" "String 3"
```

Para a API, inclua todas as strings no mesmo elemento `Value`:

```
<Value>"String 1" "String 2" "String 3"</Value>
```

O tamanho máximo de um valor em um registro TXT é de 4.000 caracteres.

Para inserir mais de um valor de TXT, insira um valor por linha.

Caracteres especiais em um valor de registro TXT

Se o registro TXT contém os caracteres a seguir, você deve especificar os caracteres usando códigos de escape no formato `\`*`código octal de três dígitos`*:

- Os caracteres 000 a 040 octal (0 a 32 decimal, 0x00 a 0x20 hexadecimal)
- Os caracteres 177 a 377 octal (127 a 255 decimal, 0x7F a 0xFF hexadecimal)

Por exemplo, se o valor do seu registro TXT é `"exämple.com"`, você especifica `"ex\344mple.com"`.

Para um mapeamento entre caracteres ASCII e códigos octais, faça uma pesquisa na Internet com "ascii octal codes." Uma referência útil é Código ASCII – A tabela ASCII estendida.

Para incluir as aspas (") em uma string, coloque um caractere de barra invertida (\) antes das aspas: \".

Maiúsculas e minúsculas em um valor de registro TXT

O uso de maiúsculas e minúsculas é preservado, portanto, "Ab" e "aB" são valores diferentes.

Exemplos

Exemplo para o console do Amazon Route 53

Coloque cada valor em uma linha separada:

```
"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"
```

Exemplo para a API do Route 53

Coloque cada valor em um elemento de Value separado:

```
<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>
```

Criar registros usando o console do Amazon Route 53

O procedimento a seguir explica como criar registros usando o console do Amazon Route 53. Para obter informações sobre como criar registros usando a API do Route 53, consulte ChangeResourceRecordSetsa Referência da API do Amazon Route 53.

> **Note**
>
> Para criar registros para configurações de roteamento complexas, você também pode usar o editor visual de fluxo de tráfego e salvar a configuração como uma política de tráfego. Em seguida, é possível associar a política de tráfego a um ou mais nomes de domínio (como example.com) ou nomes de subdomínio (como www.example.com), na mesma ou em várias zonas hospedadas. Além disso, você poderá reverter as atualizações se a nova configuração

não estiver sendo executada conforme o esperado. Para ter mais informações, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS.

Para criar um registro usando o console do Route 53

1. Se você não estiver criando um registro de alias, vá para a etapa 2.

   Além disso, vá para a etapa 2 se você estiver criando um registro de alias que roteia o tráfego DNS para um AWS recurso que não seja um balanceador de carga do Elastic Load Balancing ou outro registro do Route 53.

   Se você estiver criando um registro de alias que roteia tráfego para um balanceador de carga de Elastic Load Balancing e tiver criado a zona hospedada e o balanceador de carga usando contas diferentes, siga o procedimento Obter o nome do DNS para um balanceador de carga de Elastic Load Balancing para obter o nome DNS do balanceador de carga.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Se você já tem uma zona hospedada para seu domínio, vá para a etapa 5. Se você não tem, siga o procedimento aplicável para criar uma zona hospedada:

   - Para encaminhar o tráfego de Internet para seus recursos, como buckets do Amazon S3 ou instâncias do Amazon EC2, consulte Criar uma zona hospedada pública.
   - Para rotear o tráfego em sua VPC, consulte Criar uma zona hospedada privada.
5. Na página Hosted zones (Zonas hospedadas), escolha o nome da zona hospedada na qual deseja criar os registros.
6. Escolha Create record (Criar registro).
7. Escolha e defina valores e política de roteamento aplicáveis. Para obter mais informações, consulte o tópico para o tipo de registro que você deseja criar:

   - Valores que são comuns para todas as políticas de roteamento
   - Valores que são comuns para registros de alias em todas as políticas de roteamento
   - Valores específicos para registros simples
   - Valores específicos para registros de alias simples
   - Valores específicos para registros de failover

- Valores específicos para registros de alias de failover
- Valores específicos para registros de localização geográfica
- Valores específicos para registros de alias de localização geográfica
- Valores específicos para registros de geoproximidade
- Valores específicos para registros de alias de geoproximidade
- Valores específicos para registros de latência
- Valores específicos para registros de alias de latência
- Valores específicos para registros baseados em IP
- Valores específicos para registros de alias baseado em IP
- Valores específicos para registros de resposta com valores múltiplos
- Valores específicos para registros ponderados
- Valores específicos para registros de alias ponderados

8. Escolha Create records (Criar registros).

> **Note**
>
> Os novos registros demoram para ser propagados até os servidores DNS do Route 53. Atualmente, a única forma de verificar se as alterações se propagaram é usando a ação da GetChangeAPI. As alterações geralmente são propagadas para todos os servidores de nome do Route 53 em até 60 segundos.

9. Se você estiver criando vários registros, repita as etapas de 7 a 8.

Obter o nome do DNS para um balanceador de carga de Elastic Load Balancing

1. Faça login AWS Management Console usando a AWS conta que foi usada para criar o Classic, o Application ou o Network Load Balancer para o qual você deseja criar um registro de alias.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, selecione Load Balancers.
4. Na lista de load balancers, selecione aquele para o qual você deseja criar um registro de alias.
5. Na guia Descrição, obtenha o valor de Nome DNS.
6. Se quiser criar registros de alias para outros balanceadores de carga de Elastic Load Balancing, repita as etapas 4 e 5.

7. Saia do AWS Management Console.
8. Faça login AWS Management Console novamente usando a AWS conta que você usou para criar a zona hospedada do Route 53.
9. Volte para a etapa 3 do procedimento Criar registros usando o console do Amazon Route 53.

Permissões do conjunto de registros de recursos

As permissões do conjunto de registros de recursos usam condições de política de gerenciamento de identidade e acesso (IAM) para permitir que você defina permissões granulares para ações no console do Route 53 ou para usar a ChangeResourceRecordSetsAPI.

Um conjunto de registros de recursos é definido como vários registros de recursos com o mesmo nome e tipo (e classe, mas, para a maioria dos propósitos, a classe é sempre IN ou Internet), mas eles contêm dados diferentes. Por exemplo, se você escolher o roteamento por geolocalização, poderá ter vários registros A ou AAAA apontando para diferentes endpoints do mesmo domínio. Todos esses registros A ou AAAA se combinam para formar um conjunto de registros de recursos. Para obter mais informações sobre a terminologia DNS, consulte RFC 7719.

Com as condições da política do IAM`route53:ChangeResourceRecordSetsNormalizedRecordNames`,`route53:ChangeResourceRecord`route53:ChangeResourceRecordSetsActions, você pode conceder direitos administrativos granulares a outros AWS usuários em qualquer outra AWS conta. Isso permite que você conceda a alguém permissões para:

- Um único conjunto de registros de recursos.
- Todos os conjuntos de registros de recursos de um tipo de registro DNS específico.
- Conjuntos de registros de recursos em que os nomes contêm uma string específica.
- Execute uma ou todas as `CREATE | UPSERT | DELETE` ações ao usar a ChangeResourceRecordSetsAPI ou o console do Route 53.

Você também pode criar permissões de acesso que combinem qualquer uma das condições da política do Route 53. Por exemplo, você pode conceder a alguém permissões para modificar os dados do registro A para marketing-example.com, mas não permitir que esse usuário exclua nenhum registro.

Para obter mais informações sobre permissões de conjuntos de registros de recursos, consulte Uso de condições de política do IAM para controle de acesso refinado para gerenciar conjuntos de registros de recursos.

Para saber como autenticar AWS usuários, consulte Autenticando com identidades e saiba como controlar o acesso aos recursos do Route 53, consulteControle de acesso.

Valores que você especifica ao criar ou editar registros do Amazon Route 53

Quando você cria registros usando o console do Amazon Route 53, os valores especificados dependem da política de roteamento que você quer usar e se você está criando registros de alias, o que encaminha o tráfego para os recursos da AWS.

Tópicos

Valores que são comuns para todas as políticas de roteamento

Estes são os valores comuns que você pode especificar ao criar ou editar registros do Amazon Route 53. Eles são utilizados por todas as políticas de roteamento.

Tópicos

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Registros CNAME

Se você estiver criando um registro com um valor CNAME para o Record type (Tipo de registro), o registro não poderá ter o mesmo o nome da zona hospedada.

Caracteres especiais

Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Caracteres curinga

Você pode usar um asterisco (*) no nome. O DNS trata o caractere * como um caractere curinga ou como o caractere * (ASCII 42), dependendo de onde ele aparece no nome. Para obter mais informações, consulte Usar um asterisco (*) nos nomes de zonas hospedadas e registros.

> **Important**
>
> O curinga * não pode ser usado para conjuntos de registros de recursos que tenham um tipo NS.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

A: endereço IPv4

Um endereço IP no formato IPv4, por exemplo, 192.0.2.235.

AAAA: endereço IPv6

Um endereço IP no formato IPv6, por exemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334.

CAA: Autorização da Autoridade de Certificação

Três valores separados por vírgula que determinam quais autoridades de certificação têm permissão para emitir certificados ou certificados curinga para o domínio ou o subdomínio especificado por Record name (Nome do registro). Você pode usar registros CAA para especificar:

- Quais autoridades de certificação (CAs) podem emitir certificados SSL/TLS, se houver
- O endereço de e-mail ou o URL a ser contatado quando a CA emitir um certificado para o domínio ou o subdomínio

CNAME: Nome canônico

O nome de domínio totalmente qualificado (por exemplo, www.example.com) que você deseja que o Route 53 retorne em resposta a consultas de DNS para esse registro. Um ponto final é opcional; o Route 53 pressupõe que o nome de domínio seja totalmente qualificado. Isso significa que o Route 53 trata www.exemplo.com (sem um ponto final) e www.exemplo.com. (com um ponto final) como valores idênticos.

MX: Servidor de mensagens

Uma prioridade e um nome de domínio especificando um servidor de e-mail, por exemplo, 10 mailserver.example.com. O ponto final é tratado como opcional.

NAPTR: Ponteiro de Autoridade de Nomes

Seis configurações separadas por espaço que são usadas por aplicações DDDS (Sistema de descoberta de delegação dinâmica) para um valor para outro ou para substituir um valor por outro. Para obter mais informações, consulte Tipo de registro NAPTR.

PTR: Ponteiro

O nome de domínio que você deseja que o Route 53 retorne.

NS: servidor de nomes

O nome de domínio um servidor de nomes, por exemplo, ns1.example.com.

> **Note**
>
> É possível especificar um registro NS apenas com uma política de roteamento simples.

SPF: Framework de Política de Remetente

Um registro de SPF entre aspas exemplo, "v=spf1 ip4:192.168.0.1/16-all". Não é recomendado usar registros de SPF. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

SRV: Localizador de serviço

Um registro de SRV. Os registros de SRV são usados para acessar serviços, como um serviço para e-mail ou comunicações. Para obter informações sobre o formato de registros de SRV, consulte a documentação do serviço ao qual você deseja se conectar. O ponto final é tratado como opcional.

O formato de um registro de SRV é:

[priority] [weight] [port] [server host name] ([prioridade] [peso] [porta] [nome de host do servidor])

Por exemplo:

1 10 5269 xmpp-server.example.com.

TXT: Texto

Um registro de texto. Texto entre aspas, por exemplo, “Sample text entry” (“Exemplo de entrada de texto”).

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valores que são comuns para registros de alias em todas as políticas de roteamento

Estes são os valores de alias comuns que você pode especificar ao criar ou editar registros do Amazon Route 53. Eles são utilizados por todas as políticas de roteamento.

Tópicos

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Registros CNAME

Se você estiver criando um registro com um valor CNAME para o Type (Tipo), o registro não poderá ter o mesmo o nome da zona hospedada.

Aliases para distribuições do CloudFront e buckets do Amazon S3

O valor que você especifica depende, em partes, do recurso da AWS para o qual você está encaminhando o tráfego:

- CloudFront distribution (Distribuição do CloudFront): sua distribuição deve incluir um nome de domínio alternativo que corresponda ao nome do registro. Por exemplo, se o nome do registro for acme.example.com, sua distribuição do CloudFront deve incluir acme.example.com como um dos nomes de domínio alternativos. Para obter mais informações, consulte Como usar nomes de domínio alternativos (CNAMEs) no Guia do desenvolvedor do Amazon CloudFront.
- Bucket do Amazon S3 (Bucket do Amazon S3): o nome do registro deve corresponder ao nome de seu bucket do Amazon S3. Por exemplo, se o nome do seu bucket for acme.example.com, o nome desse registro também deve ser acme.example.com.

Além disso, você deve configurar o bucket para hospedagem de sites. Para obter mais informações, consulte o tópico sobre como Configurar um bucket para hospedagem do sites, no Guia do usuário do Amazon Simple Storage Service.

Caracteres especiais

Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Caracteres curinga

Você pode usar um asterisco (*) no nome. O DNS trata o caractere * como um caractere curinga ou como o caractere * (ASCII 42), dependendo de onde ele aparece no nome. Para obter mais informações, consulte Usar um asterisco (*) nos nomes de zonas hospedadas e registros.

Valor/rotear tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Important

Se você usou a mesma conta da AWS para criar a zona hospedada e o recurso para o qual está encaminhando tráfego, e se o recurso não for exibido na lista de Endpoints, verifique o seguinte:

- Confirme se você escolheu um valor compatível em Record type (Tipo de registro). Os valores compatíveis são específicos do recurso para o qual o tráfego está sendo roteado. Por exemplo, para encaminhar o tráfego para um bucket do S3, é necessário escolher A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro).
- Verifique se a conta tem as permissões do IAM necessárias para listar os recursos aplicáveis. Por exemplo, para que as distribuições do CloudFront sejam exibidas na lista de Endpoints, a conta deve ter permissão para executar a seguinte ação: `cloudfront:ListDistributions`.

Para ver um exemplo de política do IAM, consulte Permissões necessárias para usar o console do Amazon Route 53.

Se você usou contas diferentes da AWS para criar a zona hospedada e o recurso, a lista de Endpoints não exibe o recurso. Consulte a documentação a seguir para o tipo de recurso, a fim de determinar qual valor deve ser digitado em Endpoint.

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Para APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway, realize um dos seguintes procedimentos:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e sua API: escolha Endpoint e escolha uma API na lista. Se tiver muitas APIs, insira os primeiros caracteres do endpoint da API para filtrar a lista.

  > **Note**
  >
  > O nome desse registro deve corresponder a um nome de domínio personalizado para sua API, como api.example.com.

- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e a API: insira o endpoint da API para a API, como api.example.com.

  Se você usou uma conta da AWS para criar a zona hospedada atual e uma conta diferente para criar uma API, a API não será exibida na lista Endpoints em API Gateway APIs (APIs de API Gateway).

  Se você usou uma conta para criar a zona hospedada atual e uma ou mais contas diferentes para criar todas suas APIs, a lista Endpoints mostra No targets available (Nenhum destino disponível) em API Gateway APIs (APIs de API Gateway). Para obter mais informações, consulte Encaminhar o tráfego para uma API do Amazon API Gateway por meio do seu nome de domínio.

Distribuições do CloudFront

Para distribuições do CloudFront, realize uma das seguintes ações:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e sua distribuição do CloudFront: escolha Endpoint e escolha uma distribuição na lista. Se tiver uma grande quantidade de distribuições, você poderá inserir os primeiros caracteres do nome de domínio de sua distribuição para filtrar a lista.

  Caso sua distribuição não apareça na lista, observe o seguinte:

  - O nome do registro deve corresponder a um nome de domínio alternativo em sua distribuição.
  - Se você tiver acabado de adicionar um nome de domínio alternativo para sua distribuição, pode levar até 15 minutos para que as alterações sejam propagadas a todos os locais da borda do CloudFront. Até que as alterações tenham sido propagadas, o Route 53 não conhecerá o novo nome de domínio alternativo.
- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e sua distribuição: insira o nome de domínio do CloudFront para a distribuição, como d111111abcdef8.cloudfront.net.

  Se você tiver usado uma conta da AWS para criar a zona hospedada atual e uma conta diferente para criar uma distribuição, a distribuição não aparecerá na lista Endpoints.

  Se você usou uma conta para criar a zona hospedada atual e uma ou mais contas diferentes para criar todas as suas distribuições, a lista Endpoints mostrará No targets available (Nenhum destino disponível) em CloudFront distributions (Distribuições do CloudFront).

> **Important**
>
> Não faça roteamento de consultas para uma distribuição do CloudFront que ainda não tenha sido propagada para todos os locais da borda; caso contrário, os usuários não poderão acessar o conteúdo aplicável.

Sua distribuição do CloudFront deve incluir um nome de domínio alternativo que corresponda ao nome do registro. Por exemplo, se o nome do registro for acme.example.com, sua distribuição do CloudFront deve incluir acme.example.com como um dos nomes de domínio alternativos. Para obter mais informações, consulte Como usar nomes de domínio alternativos (CNAMEs) no Guia do desenvolvedor do Amazon CloudFront.

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA —

IPv6 address (AAAA: endereço IPv6). Para obter mais informações, consulte Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se o nome de domínio do seu ambiente do Elastic Beanstalk incluir a região na qual você implantou esse ambiente, será possível criar um registro de alias que encaminha o tráfego a esse ambiente. Por exemplo, o nome de domínio `my-environment.us-west-2.elasticbeanstalk.com` é um nome de domínio regionalizado.

> **Important**
>
> Para ambientes que foram criados antes do início de 2016, o nome do domínio não inclui a região. Para rotear o tráfego a esses ambientes, você deve criar um registro CNAME em vez de um registro de alias. Observe que não é possível criar um registro CNAME para o nome de domínio raiz. Por exemplo, se o nome de seu domínio for exemplo.com, você poderá criar um registro que direciona o tráfego de acme.exemplo.com para seu ambiente do Elastic Beanstalk, mas não poderá criar um registro que direcione o tráfego de exemplo.com para seu ambiente do Elastic Beanstalk.

Para ambientes do Elastic Beanstalk com subdomínios regionalizados, faça o seguinte:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e seu ambiente do Elastic Beanstalk: escolha Endpoint e escolha um ambiente na lista. Se tiver uma grande quantidade de ambientes, você poderá inserir os primeiros caracteres do atributo CNAME do ambiente para filtrar a lista.
- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e seu ambiente do Elastic Beanstalk: insira o atributo CNAME para o ambiente do Elastic Beanstalk.

Para obter mais informações, consulte Roteamento do tráfego para um ambiente AWS Elastic Beanstalk.

Load balancers do ELB

Para load balancers do ELB, realize uma das seguintes ações:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e seu balanceador de carga: escolha Endpoint e escolha um balanceador de carga na lista. Se tiver uma grande quantidade de load balancers, você poderá inserir os primeiros caracteres do nome de DNS para filtrar a lista.

- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e seu balanceador de carga: insira o valor que você recebeu no procedimento Obter o nome do DNS para um balanceador de carga de Elastic Load Balancing.

  Se você usou uma conta da AWS para criar a zona hospedada atual e uma conta diferente para criar um balanceador de carga, o balanceador de carga não aparecerá na lista Endpoints.

  Se você usou uma conta para criar a zona hospedada atual e uma ou mais contas diferentes para criar todos os seus balanceadores de carga, a lista Endpoints mostrará No targets available (Nenhum destino disponível) em Elastic Load Balancers (Balanceadores de carga elásticos).

O console precede dualstack. para o Application Load Balancer e o Classic Load Balancer de uma conta diferente. Quando um cliente, como um navegador, solicita o endereço IP para o seu nome de domínio (exemplo.com) ou nome do subdomain (www.exemplo.com), o cliente pode solicitar um endereço IPv4 (um registro A), um endereço IPv6 (um registro AAAA), ou ambos (em solicitações separadas). A designação dualstack permite que o Route 53 responda com o endereço IP apropriado ao seu balanceador de carga, com base no formato de endereço IP que o cliente solicitou.

Para obter mais informações, consulte Rotear tráfego para um load balancer do ELB.

Aceleradoras do AWS Global Accelerator

Para as aceleradoras do AWS Global Accelerator, insira o nome DNS da aceleradora. É possível inserir o nome DNS de uma aceleradora criada usando a conta atual da AWS ou usando outra conta da AWS.

Buckets do Amazon S3

Para buckets do Amazon S3 que estão configurados como endpoints de site, realize uma das seguintes ações:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e seu bucket do Amazon S3: escolha Endpoint e escolha um bucket da lista. Se tiver uma grande quantidade de buckets, você poderá inserir os primeiros caracteres do nome de DNS para filtrar a lista.

  O valor de Endpoint é alterado para o endpoint do site do Amazon S3 do seu bucket.
- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e seu bucket do Amazon S3: insira o nome da região na qual criou o bucket do S3. Use o valor exibido na coluna Endpoint de site na tabela Amazon S3 website endpoints no Referência geral da Amazon Web Services.

Se você usou contas da AWS diferentes da conta atual para criar os buckets do Amazon S3, o bucket não aparecerá na lista Endpoints.

Você deve configurar o bucket para hospedagem de sites. Para obter mais informações, consulte o tópico sobre como Configurar um bucket para hospedagem do sites, no Guia do usuário do Amazon Simple Storage Service.

O nome do registro deve corresponder ao nome de seu bucket do Amazon S3. Por exemplo, se o nome do seu bucket do Amazon S3 for acme.example.com, o nome desse registro também deve ser acme.example.com.

Em um grupo de registros de alias ponderado, alias de latência, alias de failover ou de alias de localização geográfica, você pode criar apenas um registro que encaminhará as consultas para um bucket do Amazon S3 porque o nome do registro deve coincidir com o nome do bucket, e os nomes de bucket devem ser globalmente exclusivos.

Endpoints de interface da Amazon VPC

Para endpoints da interface da Amazon VPC, realize um dos seguintes procedimentos:

- Se você usou a mesma conta para criar sua zona hospedada do Route 53 e seu endpoint da interface: escolha Endpoint e escolha um endpoint da interface da lista. Se tiver uma grande quantidade de endpoints de interface, insira os primeiros caracteres do nome de host de DNS para filtrar a lista.
- Se você usou contas diferentes para criar sua zona hospedada do Route 53 e seu endpoint de interface: insira o nome de host de DNS para o endpoint de interface, como vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com.

  Se você tiver usado uma conta da AWS para criar a zona hospedada atual e uma conta diferente para criar um endpoint de interface, o endpoint de interface não será exibido na lista Endpoint em VPC endpoints (Endpoints da VPC).

  Se tiver usado uma conta para criar a zona hospedada atual e uma ou mais contas diferentes para criar todos os seus endpoints de interface, a lista Endpoint mostra No targets available (Nenhum destino disponível) em VPC Endpoints (Endpoints da VPC).

  Para obter mais informações, consulte Como encaminhar o tráfego para um endpoint de interface da Amazon Virtual Private Cloud por meio do seu nome de domínio.

Registros nessa zona hospedada

Para registros nessa zona hospedada, escolha Endpoint e escolha o registro aplicável. Se tiver uma grande quantidade de registros, você poderá inserir os primeiros caracteres do nome para filtrar a lista.

Se a zona hospedada contiver apenas os registros de NS e SOA padrão, a lista de Endpoints mostrará No targets available (Nenhum destino disponível).

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível escolher um registro para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Valores específicos para registros simples

Quando você criar registros básicos, especifique os seguintes valores.

Tópicos

Política de roteamento

Escolha Simple routing (Roteamento simples).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação

- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- NS: servidor de nomes

  O nome de domínio um servidor de nomes, por exemplo, ns1.example.com.

  > **Note**
  >
  > É possível especificar um registro NS apenas com uma política de roteamento simples.

- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor para Record type (Tipo de registro) com base em como deseja que o Route 53 responda a consultas de DNS.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores

recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Valores específicos para registros de alias simples

Quando você criar registros de alias, especifique os seguintes valores. Para obter mais informações, consulte Escolher entre registros de alias e não alias.

> **Note**
>
> Se você estiver usando o Route 53 na AWS GovCloud (US) Region, esse recurso tem algumas restrições. Para obter mais informações, consulte a página do Amazon Route 53 no AWS GovCloud (US)Manual do usuário do .

Tópicos

- Política de roteamento
- Nome de registro
- Valor/rotear tráfego para
- Tipo de registro
- Avaliar status do alvo

Política de roteamento

Escolha Simple routing (Roteamento simples).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Valor/rotear tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS você pode visar, consulte valores comuns para registros de alias para os quais avaliar/rotear tráfego.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Type (Tipo) e outro com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível rotear o tráfego para um registro para o qual o valor de Type (Tipo) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Avaliar status do alvo

Quando o valor de Routing policy (Política de roteamento) é Simple (Simples), é possível escolher No (Não) ou o padrão Yes (Sim), pois a opção Evaluate target health (Avaliar integridade do destino) não tem efeito para o encaminhamento Simple (Simples). Se você tiver apenas um registro com um nome e um tipo, o Route 53 responderá às consultas de DNS usando os valores desse registro, independentemente da integridade dos recursos.

Valores específicos para registros de failover

Quando você criar registros de failover, especifique os seguintes valores.

> **Note**
>
> Para obter informações sobre como criar registros de failover em uma zona hospedada privada, consulte Configurar failover em uma zona hospedada privada.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- TTL (segundos)
- Valor/Encaminhar tráfego para
- Tipo de registro de failover
- Verificação de integridade
- ID de registro

Política de roteamento

Escolha Failover.

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para os dois registros no grupo de registros de failover.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o mesmo valor para os registros de failover primário e secundário.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação

- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Tipo de registro de failover

Escolha o valor aplicável a esse registro. Para que o failover funcione corretamente, você deve criar um nó principal e um registro de failover secundário.

Não é possível criar registros sem failover que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de failover.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica

IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.

- Selecione Yes (Sim) em Evaluate Target Health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain Name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain Name (Nome de domínio) corresponde ao nome dos registros e associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

ID de registro

Insira um valor que identifique os registros primários e secundários de forma exclusiva.

Valores específicos para registros de alias de failover

Quando você criar registros de alias de failover, especifique os seguintes valores.

Para obter informações, consulte os seguintes tópicos:

- Para obter informações sobre como criar registros de failover em uma zona hospedada privada, consulte Configurar failover em uma zona hospedada privada.
- Para obter informações sobre registros de alias, consulte Escolher entre registros de alias e não alias.

Tópicos

Política de roteamento

Escolha Failover.

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para os dois registros no grupo de registros de failover.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego. Selecione o mesmo valor para os registros de failover primário e secundário:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Type (Tipo) e outro com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível rotear o tráfego para um registro para o qual o valor de Type (Tipo) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS você pode visar, consulte valores comuns para registros de alias para os quais avaliar/rotear tráfego.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

> **Note**
>
> Ao criar registros de failover principais e secundários, você pode criar um failover e um registro de alias de failover que tenham os mesmos valores de Name (Nome) e Record type (Tipo de registro). Se você combinar registros de failover e de alias de failover, qualquer um deles pode ser um registro primário.

Tipo de registro de failover

Escolha o valor aplicável a esse registro. Para que o failover funcione corretamente, você deve criar um nó principal e um registro de failover secundário.

Não é possível criar registros sem failover que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de failover.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate Target Health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain Name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain Name (Nome de domínio) corresponde ao nome dos registros e associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API regional personalizada do API Gateway ou uma API otimizada para bordas.

Distribuições do CloudFront

Você não poderá definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma distribuição do CloudFront.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de Carga Clássico do ELB em Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas com o balanceador de carga. Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará consultas para outros recursos.
- Application and Network Load Balancers (Aplicação e Balanceadores de Carga de Rede) se você especificar uma Aplicação ou Balanceador de Carga de Rede do ELB e definir Evaluate Target health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:
  - Para que um Application ou Network Load Balancer seja considerado íntegro, um grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.
  - Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos

associar uma verificação de integridade a todos os registros no destino do endpoint. Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique os registros primários e secundários de forma exclusiva.

Valores específicos para registros de localização geográfica

Quando você criar registros de localização geográfica, especifique os seguintes valores.

Tópicos

Política de roteamento

Escolha Geolocation (Localização geográfica).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Insira o mesmo nome para todos os registros no grupo de registros de localização geográfica.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o mesmo valor para todos os registros no grupo de registros de localização geográfica.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro

- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Local

Ao configurar o Route 53 para responder às consultas de DNS com base no local de origem das consultas, selecione o continente ou país ao qual deseja que o Route 53 responda com as configurações nesse registro. Se quiser que o Route 53 responda às consultas de DNS para estados individuais nos Estados Unidos, selecione United States (Estados Unidos) na lista Location (Localização) e, depois, selecione o estado na lista Sublocation (Sublocalização).

Para uma zona hospedada privada, selecione o continente, o país ou a subdivisão da Região da AWS mais próxima em que seu recurso se encontra. Por exemplo, se seu recurso estiver em us-east-1, você poderá especificar América do Norte, Estados Unidos ou Virgínia.

> **Important**
>
> Recomendamos criar um registro de localização geográfica que tenha um valor Default (Padrão) para a Location (Localização). Esta ação abrange as localizações geográficas para as quais você não criou registros e endereços IP para os quais o Route 53 não consiga identificar uma localização. Quando você configurar o local padrão, defina o código do país como um asterisco "*".

Não é possível criar registros que não são de localização geográfica que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de localização geográfica.

Para obter mais informações, consulte Roteamento de localização geográfica.

Aqui estão os países que o Amazon Route 53 associa a cada continente. Os códigos de país são da ISO 3166. Para mais informações sobre o artigo da Wikipedia, consulte ISO 3166-1 alpha-2:

África (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

Antártica (AN)

AQ, GS, TF

Ásia (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

América do Norte (AN)

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

América do Sul (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

Note

O Route 53 não oferece suporte para a criação de registros de localização geográfica para os seguintes países: Ilha Bouvet (BV), Ilha Christmas (CX), Saara Ocidental (EH) e Ilha Heard e Ilhas McDonald (HM). Não há dados disponíveis sobre endereços IP para esses países.

Estados dos EUA

Ao configurar o Route 53 para responder às consultas de DNS baseadas no estado de origem das consultas provenientes dos Estados Unidos, selecione o estado na lista Estados dos EUA. Os territórios dos Estados Unidos (por exemplo, Porto Rico) são listados como países na lista Location (Localização).

> **Important**
>
> Alguns endereços IP são associados aos Estados Unidos, mas não com um estado individual. Se você criar registros para todos os estados nos Estados Unidos, recomendamos criar também um registro para os Estados Unidos para direcionar as consultas para esses endereços IP não associados. Se você não criar um registro para os Estados Unidos, o Route 53 responderá a consultas de DNS de endereços IP dos Estados Unidos não associados com as configurações de um registro de localização geográfica padrão (se você tiver criado um) ou com uma resposta de "sem resposta".

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de

um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.

- Selecione Yes (Sim) em Evaluate Target Health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain Name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain Name (Nome de domínio) corresponde ao nome dos registros e associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Para registros de localização geográfica, se um endpoint não for íntegro, o Route 53 procurará um registro para a região geográfica associada de maior tamanho. Por exemplo, digamos que você tem registros para um estado nos Estados Unidos, para os Estados Unidos, para a América do Norte e para todas as localizações (Location (Localização) é Default (Padrão)). Se o endpoint do registro de estado não estiver íntegro, o Route 53 verificará os registros para os Estados Unidos, para a América do Norte e todas as localidades, nessa ordem, até encontrar um registro que tenha um endpoint íntegro. Se todos os registros aplicáveis não estiverem íntegros, incluindo o registro para todas as localizações, o Route 53 responderá à consulta de DNS usando o valor do registro da menor região geográfica.

ID de registro

Insira um valor que identifique esse registro no grupo de registros de localização geográfica de forma exclusiva.

Valores específicos para registros de alias de localização geográfica

Quando você criar registros de alias de localização geográfica, especifique os seguintes valores.

Para obter mais informações, consulte Escolher entre registros de alias e não alias.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- Valor/Encaminhar tráfego para
- Local
- Estados dos EUA
- Verificação de integridade
- Avaliar status do alvo
- ID de registro

Política de roteamento

Escolha Geolocation (Localização geográfica).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros de localização geográfica.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego. Selecione o mesmo valor para todos os registros no grupo de registros de localização geográfica:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível encaminhar o tráfego para um registro para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o

registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS podem ser marcados, consulte Valor/rotear tráfego para.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Local

Ao configurar o Route 53 para responder às consultas de DNS com base no local de origem das consultas, selecione o continente ou país ao qual deseja que o Route 53 responda com as configurações nesse registro. Se quiser que o Route 53 responda às consultas de DNS para estados individuais nos Estados Unidos, selecione United States (Estados Unidos) na lista Location (Localização) e, depois, selecione o estado na lista U. S. states (Estados dos EUA).

Para uma zona hospedada privada, selecione o continente, o país ou a subdivisão da Região da AWS mais próxima em que seu recurso se encontra. Por exemplo, se seu recurso estiver em us-east-1, você poderá especificar América do Norte, Estados Unidos ou Virgínia.

Important

Recomendamos criar um registro de localização geográfica que tenha um valor Default (Padrão) para a Location (Localização). Esta ação abrange as localizações geográficas para as quais você não criou registros e endereços IP para os quais o Route 53 não consiga identificar uma localização. Quando você configurar o local padrão, defina o código do país como um asterisco “*”.

Não é possível criar registros que não são de localização geográfica que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de localização geográfica.

Para obter mais informações, consulte Roteamento de localização geográfica.

Aqui estão os países que o Amazon Route 53 associa a cada continente. Os códigos de país são da ISO 3166. Para mais informações sobre o artigo da Wikipedia, consulte ISO 3166-1 alpha-2:

África (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

Antártica (AN)

AQ, GS, TF

Ásia (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

América do Norte (AN)

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

América do Sul (SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> O Route 53 não oferece suporte para a criação de registros de localização geográfica para os seguintes países: Ilha Bouvet (BV), Ilha Christmas (CX), Saara Ocidental (EH) e Ilha

Heard e Ilhas McDonald (HM). Não há dados disponíveis sobre endereços IP para esses países.

Estados dos EUA

Ao configurar o Route 53 para responder às consultas de DNS baseadas no estado de origem das consultas provenientes dos Estados Unidos, selecione o estado na lista Estados dos EUA. Os territórios dos Estados Unidos (por exemplo, Porto Rico) são listados como países na lista Location (Localização).

Important

Alguns endereços IP são associados aos Estados Unidos, mas não com um estado individual. Se você criar registros para todos os estados nos Estados Unidos, recomendamos criar também um registro para os Estados Unidos para direcionar as consultas para esses endereços IP não associados. Se você não criar um registro para os Estados Unidos, o Route 53 responderá a consultas de DNS de endereços IP dos Estados Unidos não associados com as configurações de um registro de localização geográfica padrão (se você tiver criado um) ou com uma resposta de "sem resposta".

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Para registros de localização geográfica, se um endpoint não for íntegro, o Route 53 procurará um registro para a região geográfica associada de maior tamanho. Por exemplo, digamos que você tem registros para um estado nos Estados Unidos, para os Estados Unidos, para a América do Norte e para todas as localizações (Location (Localização) é Default (Padrão)). Se o endpoint do registro de estado não estiver íntegro, o Route 53 verificará os registros para os Estados Unidos, para a América do Norte e todas as localidades, nessa ordem, até encontrar um registro que tenha um endpoint íntegro. Se todos os registros aplicáveis não estiverem íntegros, incluindo o registro para todas as

localizações, o Route 53 responderá à consulta de DNS usando o valor do registro da menor região geográfica.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API Regional personalizada do API Gateway ou uma API otimizada para borda.

Distribuições do CloudFront

Você não poderá definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma distribuição do CloudFront.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de carga clássico do ELB no Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas no balanceador de carga. Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará consultas para outros recursos.

- Application and Network Load Balancers (Aplicação e Balanceadores de carga da rede): se você especificar uma Aplicação de ELB ou Balanceador de carga da rede e definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:
  - Para que um Application ou Network Load Balancer seja considerado íntegro, cada grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.
  - Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos associar uma verificação de integridade a todos os registros no destino do endpoint. Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique esse registro no grupo de registros de localização geográfica de forma exclusiva.

Valores específicos para registros de geoproximidade

Ao criar registros de geoproximidade, você especifica os seguintes valores.

Tópicos

Política de roteamento

Escolha Geoproximidade.

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Insira o mesmo nome para todos os registros no grupo de registros de geoproximidade.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para ter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o mesmo valor para todos os registros no grupo de registros de geoproximidade.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para ter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro

- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Local do endpoint

Você pode especificar a localização do endpoint do recurso usando uma das seguintes opções:

Coordenadas personalizadas

Especifique a longitude e a latitude de uma área geográfica.

Região da AWS

Escolha uma região disponível na lista de localizações.

Para obter mais informações sobre as regiões, consulte Infraestrutura AWS global.

AWSGrupo de zonas locais

Escolha um grupo de zonas locais disponível na lista de localização.

Para obter mais informações sobre Zonas Locais, consulte Zonas Locais Disponíveis no Guia do Usuário de Zonas AWS Locais. Um grupo de zonas local geralmente é a zona local sem o caractere final. Por exemplo, se a zona local for, `us-east-1-bue-1a` o grupo de zonas locais será`us-east-1-bue-1`.

Você também pode identificar o Grupo de Zonas Locais para uma zona local específica usando o 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"
```

Esse comando retorna:`"GroupName": "us-west-2-den-1"`, especificando que a zona local `us-west-2-den-1a` pertence ao grupo `us-west-2-den-1` de zonas locais.

Você não pode criar registros que não sejam de geoproximidade que tenham os mesmos valores para nome e tipo de registro que os registros de geoproximidade.

Você também não pode criar dois conjuntos de registros de recursos de geoproximidade que especifiquem o mesmo local para o mesmo nome e tipo de registro.

Viés

Um viés expande ou reduz uma área geográfica a partir da qual o Route 53 direciona o tráfego para um recurso. Um viés positivo expande a área e um viés negativo a reduz. Para ter mais informações, consulte Como o Amazon Route 53 usa o desvio para encaminhar o tráfego.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Você seleciona Sim para Evaluate Target Health para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de geoproximidade, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para ter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain Name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain Name (Nome de domínio) corresponde ao nome dos registros e associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Para registros de geoproximidade, se um endpoint não estiver íntegro, o Route 53 procurará um endpoint mais próximo que ainda esteja íntegro.

ID de registro

Insira um valor que identifique exclusivamente esse registro no grupo de registros de geoproximidade.

Valores específicos para registros de alias de geoproximidade

Ao criar registros de alias de geoproximidade, você especifica os seguintes valores.

Para ter mais informações, consulte Escolher entre registros de alias e não alias.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- Valor/Encaminhar tráfego para
- Local do endpoint
- Viés
- Verificação de integridade
- Avaliar status do alvo
- ID de registro

Política de roteamento

Escolha Geoproximidade.

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros de geoproximidade.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para ter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego. Selecione o mesmo valor para todos os registros no grupo de registros de geoproximidade:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

CloudFront distribuição

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível encaminhar o tráfego para um registro

para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS podem ser marcados, consulte Valor/rotear tráfego para.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Local do endpoint

Você pode especificar a localização do endpoint do recurso usando uma das seguintes opções:

Coordenadas personalizadas

Especifique a longitude e a latitude de uma área geográfica.

Região da AWS

Escolha uma região disponível na lista de localizações.

Para obter mais informações sobre as regiões, consulte Infraestrutura AWS global.

AWSGrupo de zonas locais

Escolha uma região de zona local disponível na lista de localização.

Para obter mais informações sobre Zonas Locais, consulte Zonas Locais Disponíveis no Guia do Usuário de Zonas AWS Locais. Um grupo de zonas local geralmente é a zona local sem o caractere final. Por exemplo, se a zona local for, `us-east-1-bue-1a` o grupo de zonas locais será`us-east-1-bue-1`.

Você também pode identificar o Grupo de Zonas Locais para uma zona local específica usando o 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"
```

Esse comando retorna:`"GroupName": "us-west-2-den-1"`, especificando que a zona local `us-west-2-den-1a` pertence ao grupo `us-west-2-den-1` de zonas locais.

Você não pode criar registros que não sejam de geoproximidade que tenham os mesmos valores para nome e tipo de registro que os registros de geoproximidade.

Você também não pode criar dois conjuntos de registros de recursos de geoproximidade que especifiquem o mesmo local para o mesmo nome e tipo de registro.

Para obter mais informações, consulte available-local-zones .html

Viés

Um viés expande ou reduz uma área geográfica a partir da qual o Route 53 direciona o tráfego para um recurso. Um viés positivo expande a área e um viés negativo a reduz. Para ter mais informações, consulte Como o Amazon Route 53 usa o desvio para encaminhar o tráfego.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de

um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.

- Você seleciona Sim para Avaliar a integridade do alvo para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de geoproximidade, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para ter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Para registros de geoproximidade, se um endpoint não estiver íntegro, o Route 53 procurará um endpoint mais próximo que ainda esteja íntegro.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API Regional personalizada do API Gateway ou uma API otimizada para borda.

CloudFront distribuições

Você não pode definir Avaliar a integridade do alvo como Sim quando o endpoint é uma CloudFront distribuição.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de carga clássico do ELB no Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas no balanceador de carga. Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará consultas para outros recursos.
- Application and Network Load Balancers (Aplicação e Balanceadores de carga da rede): se você especificar uma Aplicação de ELB ou Balanceador de carga da rede e definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:
  - Para que um Application ou Network Load Balancer seja considerado íntegro, cada grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer

grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.

- Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos associar uma verificação de integridade a todos os registros no destino do endpoint. Para ter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique esse registro de forma exclusiva no grupo de registros de geoproximidade.

Valores específicos para registros de latência

Quando você criar registros de latência, especifique os seguintes valores.

Tópicos

Política de roteamento

Escolha Latency (Latência).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros de latência.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor para Type (Tipo) com base em como deseja que o Route 53 responda a consultas de DNS.

Selecione o mesmo valor para todos os registros no grupo de registros de latência.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- CNAME: Nome canônico
- MX: Intercâmbio de mensagens

- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Região

A região do Amazon EC2 onde reside o recurso especificado nesse registro. O Route 53 recomenda uma região do Amazon EC2 com base em outros valores especificados. Isso também se aplica a zonas hospedadas privadas. Recomendamos não alterar esse valor.

Observe o seguinte:

- Só será possível criar um registro de latência para cada região do Amazon EC2.
- Não é necessário para criar registros de latência para todas as regiões do Amazon EC2. O Route 53 seleciona a região com a melhor latência entre as regiões para as quais você cria registros de latência.
- Não é possível criar registros sem latência que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de latência.
- Se você criar um registro marcado com a região cn-north-1, o Route 53 sempre responderá às consultas provenientes da China usando esse registro, independentemente da latência.

Para obter mais informações sobre como usar de latência, consulte Roteamento baseado em latência.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade

de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

ID de registro

Insira um valor que identifique esse registro no grupo de registros de latência de forma exclusiva.

Valores específicos para registros de alias de latência

Quando você criar registros de alias de latência, especifique os seguintes valores.

Para obter mais informações, consulte Escolher entre registros de alias e não alias.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- Valor/Encaminhar tráfego para
- Região
- Verificação de integridade
- Avaliar status do alvo
- ID de registro

Política de roteamento

Escolha Latency (Latência).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros de latência.

Para obter mais informações sobre nomes de registros, consulte Nome de registro

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível encaminhar o tráfego para um registro para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Selecione o mesmo valor para todos os registros no grupo de registros de latência.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS você pode visar, consulte valores comuns para registros de alias para os quais avaliar/rotear tráfego.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Região

A região do Amazon EC2 onde reside o recurso especificado nesse registro. O Route 53 recomenda uma região do Amazon EC2 com base em outros valores especificados. Isso também se aplica a zonas hospedadas privadas. Recomendamos não alterar esse valor.

Observe o seguinte:

- Só será possível criar um registro de latência para cada região do Amazon EC2.
- Não é necessário para criar registros de latência para todas as regiões do Amazon EC2. O Route 53 seleciona a região com a melhor latência entre as regiões para as quais você cria registros de latência.
- Não é possível criar registros sem latência que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros de latência.
- Se você criar um registro marcado com a região cn-north-1, o Route 53 sempre responderá às consultas provenientes da China usando esse registro, independentemente da latência.

Para obter mais informações sobre como usar de latência, consulte Roteamento baseado em latência.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade

de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain Name (Nome de domínio) corresponde ao nome dos registros e associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API regional personalizada do API Gateway ou uma API otimizada para bordas.

Distribuições do CloudFront

Você não poderá definir Evaluate Target Health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma distribuição do CloudFront.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de carga clássico do ELB no Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas no balanceador de carga. Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará consultas para outros recursos.
- Application and Network Load Balancers (Aplicação e Balanceadores de carga da rede): se você especificar uma Aplicação de ELB ou Balanceador de carga da rede e definir Evaluate

target health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:

- Para que um Application ou Network Load Balancer seja considerado íntegro, cada grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.
- Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos associar uma verificação de integridade a todos os registros no destino do endpoint. Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique esse registro no grupo de registros de latência de forma exclusiva.

Valores específicos para registros baseados em IP

Quando você criar registros baseados em IP, especifique os valores a seguir.

> **Note**
>
> Embora a criação de registros baseados em IP em uma zona hospedada privada seja permitida, não é compatível.

Tópicos

Política de roteamento

Escolha IP-based (Baseado em IP).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros baseados em IP.

Registros CNAME

Se você estiver criando um registro com um valor CNAME para o Record type (Tipo de registro), o registro não poderá ter o mesmo o nome da zona hospedada.

Caracteres especiais

Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Caracteres curinga

Você pode usar um asterisco (*) no nome. O DNS trata o caractere * como um caractere curinga ou como o caractere * (ASCII 42), dependendo de onde ele aparece no nome. Para obter mais informações, consulte Usar um asterisco (*) nos nomes de zonas hospedadas e registros.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor para Type (Tipo) com base em como deseja que o Route 53 responda a consultas de DNS.

Selecione o mesmo valor para todos os registros no grupo de registros de latência.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou

subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte Valor/Encaminhar tráfego para valores comuns para os quais avaliar/rotear tráfego.

Local

O nome do local CIDR onde o recurso especificado neste registro é especificado pelos valores de bloco CIDR no local CIDR.

Para obter mais informações sobre o uso de registros baseados em IP Roteamento baseado em IP.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias baseado em IP, alias de latência ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

ID de registro

Insira um valor que identifique exclusivamente esse registro no grupo de registros baseados em IP.

Valores específicos para registros de alias baseado em IP

Quando você criar registros de alias baseado em IP, especifique os valores a seguir.

> **Note**
>
> Embora a criação de registros de alias baseado em IP em uma zona hospedada privada seja permitida, não é compatível.

Para obter mais informações, consulte Escolher entre registros de alias e não alias.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- Valor/Encaminhar tráfego para
- Local
- Verificação de integridade
- Avaliar status do alvo
- ID de registro

Política de roteamento

Escolha IP-based (Baseado em IP).

> **Note**
>
> Embora a criação de registros de alias baseado em IP em uma zona hospedada privada seja permitida, não é compatível.

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros baseados em IP.

Registros CNAME

Se você estiver criando um registro com um valor CNAME para o Record type (Tipo de registro), o registro não poderá ter o mesmo o nome da zona hospedada.

Aliases para distribuições do CloudFront e buckets do Amazon S3

O valor que você especifica depende, em partes, do recurso da AWS para o qual você está encaminhando o tráfego:

- CloudFront distribution (Distribuição do CloudFront): sua distribuição deve incluir um nome de domínio alternativo que corresponda ao nome do registro. Por exemplo, se o nome do registro for acme.example.com, sua distribuição do CloudFront deve incluir acme.example.com como um dos nomes de domínio alternativos. Para obter mais informações, consulte Como usar nomes de domínio alternativos (CNAMEs) no Guia do desenvolvedor do Amazon CloudFront.
- Bucket do Amazon S3 (Bucket do Amazon S3): o nome do registro deve corresponder ao nome de seu bucket do Amazon S3. Por exemplo, se o nome do seu bucket for acme.example.com, o nome desse registro também deve ser acme.example.com.

  Além disso, você deve configurar o bucket para hospedagem de sites. Para obter mais informações, consulte o tópico sobre como Configurar um bucket para hospedagem do sites, no Guia do usuário do Amazon Simple Storage Service.

Caracteres especiais

Para obter informações sobre como especificar caracteres que não sejam a-z, 0-9 e - (hífen) e como especificar nomes de domínio internacionalizados, consulte Formato de nome de domínio DNS.

Caracteres curinga

Você pode usar um asterisco (*) no nome. O DNS trata o caractere * como um caractere curinga ou como o caractere * (ASCII 42), dependendo de onde ele aparece no nome. Para obter mais informações, consulte Usar um asterisco (*) nos nomes de zonas hospedadas e registros.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego. Selecione o mesmo valor para todos os registros no grupo de registros baseados em IP:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível encaminhar o tráfego para um registro

para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS você pode visar, consulte valores comuns para registros de alias para os quais avaliar/rotear tráfego.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Local

Quando configurar o Route 53 para responder a consultas ao DNS com base no local de origem das consultas, selecione o local CIDR ao qual deseja que o Route 53 responda com as configurações desse registro.

> **Important**
>
> Recomendamos criar um registro baseado em IP que tenha um valor Default (Padrão) para Location (Local). Essa ação abrange os locais para os quais você não criou registros e endereços IP para os quias o Route 53 não consegue identificar um local.

Não é possível criar registros não baseados em IP que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros baseados em IP.

Para obter mais informações, consulte Roteamento baseado em IP.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de roteamento baseado em PI, alias de latência ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Para registros de alias baseados em IP, se um endpoint não estiver íntegro, o Route 53 procurará um registro no local associado mais amplo. Por exemplo, digamos que você tem registros para um estado nos Estados Unidos, para os Estados Unidos, para a América do Norte e para todas as localizações (Location (Localização) é Default (Padrão)). Se o endpoint do registro de estado não estiver íntegro, o Route 53 verificará os registros para os Estados Unidos, para a América do Norte e todas as localidades, nessa ordem, até encontrar um registro que tenha um endpoint íntegro. Se todos os registros aplicáveis não estiverem íntegros, incluindo o registro para todas as localizações, o Route 53 responderá à consulta de DNS usando o valor do registro da menor região geográfica.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API regional personalizada do API Gateway ou uma API otimizada para bordas.

Distribuições do CloudFront

Você não poderá definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma distribuição do CloudFront.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim)

e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de carga clássico do ELB no Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas no balanceador de carga. Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará consultas para outros recursos.
- Application and Network Load Balancers (Aplicação e Balanceadores de carga da rede): se você especificar uma Aplicação de ELB ou Balanceador de carga da rede e definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:
  - Para que um Application ou Network Load Balancer seja considerado íntegro, cada grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.
  - Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos associar uma verificação de integridade a todos os registros no destino do endpoint. Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique exclusivamente esse registro no grupo de registros baseados em IP.

Valores específicos para registros de resposta com valores múltiplos

Quando você criar conjuntos de recursos com valores múltiplos, especifique os seguintes valores.

> **Note**
>
> Não há suporte para a criação de recursos de alias de resposta com valores múltiplos.

Tópicos

- Política de roteamento
- Nome de registro
- Tipo de registro
- TTL (segundos)
- Valor/Encaminhar tráfego para
- Verificação de integridade
- ID de registro

Política de roteamento

Escolha Multivalue answer (Resposta com valores múltiplos).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros do grupo de registros multivalores.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione qualquer valor, exceto NS ou CNAME.

Selecione o mesmo valor para todos os registros no grupo de registros de resposta de valores múltiplos.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

> **Note**
>
> Se você criar dois ou mais registros de resposta com vários valores que possuem o mesmo nome e tipo, estiver usando o console e especificar valores diferentes para TTL, o Route 53 alterará o valor de TTL de todos os registros para o último valor especificado.

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Se você inserir mais de um valor, insira cada um dos valores em linhas separadas.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) para Evaluate target health (Avaliar integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de localização geográfica, alias de latência ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

ID de registro

Insira um valor que identifique esse registro no grupo de registros de resposta de valores múltiplos de forma exclusiva.

Valores específicos para registros ponderados

Quando você criar registros ponderados, especifique os seguintes valores.

Tópicos

Política de roteamento

Selecione Weighted (Ponderado).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Record name (Nome de registro).

Insira o mesmo nome para todos os registros no grupo de registros ponderados.

Para obter mais informações sobre nomes de registros, consulte Nome de registro.

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o mesmo valor para todos os registros no grupo de registros ponderados.

TTL (segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172800 segundos ou dois dias), reduzirá o número de chamadas que os resolvedores recursivos de DNS devem fazer ao Route 53 para obter as informações mais recentes neste registro. Isso tem o efeito de reduzir a latência e reduzir sua fatura para o serviço do Route 53. Para obter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

No entanto, se você especificar um valor mais longo para TTL, levará mais tempo para que as alterações no registro (por exemplo, um novo endereço IP) entrem em vigor porque os resolvedores recursivos usam os valores em cache por períodos mais longos antes de solicitar as informações mais recentes ao Route 53. Se você estiver alterando as configurações de um domínio ou subdomínio que já está em uso, recomendamos que especifique inicialmente um valor mais curto, como 300 segundos, e aumente o valor depois de confirmar que as novas configurações estão corretas.

Se você estiver associando esse registro a uma verificação de integridade, recomendamos especificar um TTL de 60 segundos ou menos para que os clientes respondam rapidamente a alterações no status de integridade.

É necessário especificar o mesmo valor de TTL para todos os registros nesse grupo de registros ponderados.

> **Note**
>
> Se você criar dois ou mais registros ponderados que tenham o mesmo nome e tipo, e especificar valores diferentes para TTL, o Route 53 alterará o valor de TTL de todos os registros para o último valor que você tiver especificado.

Se um grupo de registros ponderados incluir um ou mais registro de alias ponderados que estiverem roteando um load balancer do ELB, recomendamos especificar um TTL de 60 segundos para todos os registros ponderados não de alias que tenham o mesmo nome e tipo. Valores diferentes de 60 segundos (o TTL para load balancers) alterarão o efeito dos valores especificados para Weight (Peso).

Valor/Encaminhar tráfego para

Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira um valor que seja adequado para o valor de Record type (Tipo de registro). Para todos os tipos exceto CNAME, é possível incorporar mais de um valor. Insira cada valor em uma linha separada.

Você pode direcionar tráfego ou especificar os seguintes valores:

- A: endereço IPv4
- AAAA: endereço IPv6
- CAA: Autorização da Autoridade de Certificação
- CNAME: Nome canônico
- MX: Intercâmbio de mensagens
- NAPTR: Ponteiro de Autoridade de Nomes
- PTR: Ponteiro
- SPF: Framework de Política de Remetente
- SRV: Localizador de serviço
- TXT: Texto

Para obter mais informações sobre os valores acima, consulte valores comuns para os quais avaliar/rotear tráfego.

Peso

Um valor que determina a proporção de consultas de DNS às quais o Route 53 responde para usar o registro atual. O Route 53 calcula a soma dos pesos para os registros que tenham a mesma combinação de nome de DNS e tipo. Depois, o Route 53 responde a consultas com base na proporção de um peso de um recurso em relação ao total.

Não é possível criar registros não ponderados que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros ponderados.

Insira um número inteiro entre 0 e 255. Para desabilitar o encaminhamento para um recurso, defina Weight (Peso) como 0. Se Weight (Peso) for definido como 0 para todos os registros no grupo, o tráfego será roteado para todos os recursos com probabilidade igual. Isso garante que você não desative acidentalmente o roteamento para um grupo de registros ponderados.

O efeito de configurar Weight (Peso) como 0 é diferente quando as verificações de integridade são associadas com registros ponderados. Para obter mais informações, consulte Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint.

Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

ID de registro

Insira um valor que identifique esse registro no grupo de registros ponderados de forma exclusiva.

Valores específicos para registros de alias ponderados

Quando você criar registros de alias ponderados, especifique os seguintes valores. Para obter mais informações, consulte Escolher entre registros de alias e não alias.

Tópicos

Política de roteamento

Escolha Weighted (Ponderado).

Nome de registro

Digite o nome de domínio ou do subdomínio para o qual deseja rotear o tráfego. O valor padrão é o nome da hosted zone.

> **Note**
>
> Se você estiver criando um registro que tenha o mesmo nome que a zona hospedada, não insira um valor (por exemplo, um símbolo de @) no campo Name (Nome).

Insira o mesmo nome para todos os registros no grupo de registros ponderados.

Para obter mais informações sobre nomes de registros, consulte Nome de registro

Tipo de registro

O tipo de registro de DNS. Para obter mais informações, consulte Tipos de registro de DNS com suporte.

Selecione o valor aplicável, baseado no recurso da AWS para o qual estiver roteando o tráfego:

API regional personalizada do API Gateway ou API otimizada para bordas

Selecione A — IPv4 address (A: endereço IPv4).

Endpoints de interface da Amazon VPC

Selecione A — IPv4 address (A: endereço IPv4).

Distribuição do CloudFront

Selecione A — IPv4 address (A: endereço IPv4).

Se IPv6 estiver habilitado para a distribuição, crie dois registros, um com um valor de A — IPv4 address (A: endereço IPv4) para Record type (Tipo de registro) e um com um valor de AAAA — IPv6 address (AAAA: endereço IPv6).

Ambiente do Elastic Beanstalk com subdomínios regionalizados

Selecione A — IPv4 address (A: endereço IPv4)

Load balancer ELB

Selecione A — IPv4 address (A: endereço IPv4) ou AAAA — IPv6 address (AAAA: endereço IPv6)

Bucket do Amazon S3

Selecione A — IPv4 address (A: endereço IPv4)

Outro registro nessa zona hospedada

Selecione o tipo de registro para o qual está criando o alias. Todos os tipos são compatíveis, exceto NS e SOA.

> **Note**
>
> Se você estiver criando um registro de alias com o mesmo nome da zona hospedada (conhecida como apex de zona), não será possível encaminhar o tráfego para um registro para o qual o valor de Record type (Tipo de registro) seja CNAME. Isso ocorre porque o registro de alias deve ter o mesmo tipo que o registro para o qual você está roteando o tráfego e não há suporte para criar um registro CNAME para o apex de zona mesmo para um registro de alias.

Selecione o mesmo valor para todos os registros no grupo de registros ponderados.

Valor/Encaminhar tráfego para

O valor escolhido na lista ou digitado no campo depende do recurso da AWS para o qual o tráfego está sendo roteado.

Para obter informações sobre quais recursos da AWS você pode visar, consulte valores comuns para registros de alias para os quais avaliar/rotear tráfego.

Para saber mais sobre como configurar o Route 53 para encaminhar o tráfego em direção a recursos da AWS específicos, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Peso

Um valor que determina a proporção de consultas de DNS às quais o Route 53 responde para usar o registro atual. O Route 53 calcula a soma dos pesos para os registros que tenham a mesma combinação de nome de DNS e tipo. Depois, o Route 53 responde a consultas com base na proporção de um peso de um recurso em relação ao total.

Não é possível criar registros não ponderados que tenham os mesmos valores para Record name (Nome do registro) e Record type (Tipo de registro) que os registros ponderados.

Insira um número inteiro entre 0 e 255. Para desabilitar o encaminhamento para um recurso, defina Weight (Peso) como 0. Se Weight (Peso) for definido como 0 para todos os registros no grupo, o tráfego será roteado para todos os recursos com probabilidade igual. Isso garante que você não desative acidentalmente o roteamento para um grupo de registros ponderados.

O efeito de configurar Weight (Peso) como 0 é diferente quando as verificações de integridade são associadas com registros ponderados. Para obter mais informações, consulte Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada.

Verificação de integridade

Selecione uma verificação de integridade, se quiser que o Route 53 verifique a integridade de um endpoint especificado e responda a consultas de DNS usando esse registro somente quando o endpoint for íntegro.

O Route 53 não verifica a integridade do endpoint especificado no registro, por exemplo, o endpoint especificado pelo endereço IP no campo Value (Valor). Ao selecionar uma verificação de integridade

de um registro, o Route 53 verifica a integridade do endpoint especificado na verificação de integridade. Para obter informações sobre como o Route 53 determina se um endpoint é íntegro, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Associar uma verificação de integridade a um registro é útil somente quando o Route 53 estiver escolhendo entre dois ou mais registros para responder a uma consulta de DNS, e você desejar que o Route 53 baseie a escolha, em parte, no status de uma verificação de integridade. Use as verificações de integridade somente nas seguintes configurações:

- Você está verificando a integridade de todos os registros em um grupo de registros que tem o mesmo nome, tipo e política de roteamento (como failover ou registros ponderados) e especifica IDs de verificação de integridade para todos os registros. Se a verificação de integridade de um registro especificar um endpoint que não esteja íntegro, o Route 53 para de responder às consultas, usando o valor para esse registro.
- Selecione Yes (Sim) em Evaluate target health (Avaliar a integridade do destino) para um registro de alias ou os registros em um grupo de alias de failover, alias de geolocalização, alias de latência, alias baseado em IP ou registro de alias ponderado. Se o registro de alias fizer referência a registros não de alias na mesma zona hospedada, você também deve especificar as verificações de integridade para os registros mencionados. Se você associar uma verificação de integridade a um registro de alias e também selecionar Yes (SIM) para Evaluate Target Health (Avaliar integridade do destino), ambos devem ser avaliados como verdadeiros. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.

Se suas verificações de integridade especificarem o endpoint apenas por nome de domínio, recomendamos que você crie uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name (Nome de domínio), especifique o nome do domínio do servidor (como us-east-2-www.exemplo.com), não o nome dos registros (www.exemplo.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Avaliar status do alvo

Selecione Yes (Sim), se quiser que o Route 53 determine se deve responder a consultas de DNS usando esse registro, verificando a integridade do recurso especificado pelo Endpoint.

Observe o seguinte:

APIs regionais personalizadas e APIs otimizadas para bordas do API Gateway

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma API Regional personalizada do API Gateway ou uma API otimizada para borda.

Distribuições do CloudFront

Você não poderá definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for uma distribuição do CloudFront.

Ambientes do Elastic Beanstalk com subdomínios regionalizados

Se você especificar um ambiente do Elastic Beanstalk no Endpoint e o ambiente contiver um load balancer do ELB, o Elastic Load Balancing encaminhará consultas apenas para as instâncias íntegras do Amazon EC2 que estão registradas com o balanceador de carga. (Um ambiente contém automaticamente um load balancer do ELB se incluir mais de uma instância do Amazon EC2.) Se você definir Evaluate target health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do Amazon EC2 estiver íntegro ou o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará as consultas para outros recursos disponíveis que sejam íntegros, se houver.

Se o ambiente contiver uma única instância do Amazon EC2, não há requisitos especiais.

Load balancers ELB

O comportamento de verificação da integridade depende do tipo do load balancer:

- Classic Load Balancers (Balanceadores de carga clássicos): se você especificar um Balanceador de carga clássico do ELB no Endpoint, o Elastic Load Balancing encaminhará consultas apenas para instâncias do Amazon EC2 íntegras que estejam registradas no balanceador de carga. Se você definir Evaluate Target Health (Avaliar integridade do destino) como Yes (Sim) e nenhuma instância do EC2 estiver íntegra, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminha consultas para outros recursos.
- Application e Network Load Balancers (Aplicação e Balanceadores de Carga de Rede): se você especificar uma Aplicação ou Balanceador de Carga de Rede do ELB e definir Evaluate Target

Health (Avaliar integridade do destino) como Yes (Sim), o Route 53 encaminha consultas para o balanceador de carga com base na integridade dos grupos de destino que estão associados com o balanceador de carga:

- Para que um Application ou Network Load Balancer seja considerado íntegro, cada grupo de destino que contenha destinos deve conter pelo menos um destino íntegro. Se qualquer grupo de destinos contiver somente destinos não íntegros, o load balancer será considerado não íntegro e o Route 53 direcionará as consultas para outros recursos.
- Um grupo de destinos que não tenha destinos registrados é considerado não íntegro.

> **Note**
>
> Ao criar um load balancer, defina as configurações para verificações de integridade do Elastic Load Balancing; elas não são verificações de integridade do Route 53, mas executam uma função semelhante. Não crie verificações de integridade do Route 53 para as instâncias do EC2 registradas com um load balancer do ELB.

Buckets do S3

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um bucket do S3.

Endpoints de interface da Amazon VPC

Não existem requisitos especiais para configurar Evaluate target health (Avaliar integridade do destino) como Yes (Sim) quando o endpoint for um endpoint da interface da Amazon VPC.

Outros registros na mesma zona hospedada

Se o recurso da AWS especificado em Endpoint for um registro ou um grupo de registros (por exemplo, um grupo de registros ponderados), mas não for outro registro de alias, recomendamos associar uma verificação de integridade a todos os registros no destino do endpoint. Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?.

ID de registro

Insira um valor que identifique esse registro no grupo de registros ponderados de forma exclusiva.

Criar registros importando um arquivo de zona

Se você estiver migrando de outro provedor de serviço de DNS, e se o provedor de serviço de DNS atual permitir que você exporte suas configurações de DNS atuais para um arquivo de zona, você poderá criar rapidamente todos os registros para uma zona hospedada do Amazon Route 53 importando um arquivo de zona.

> **Note**
>
> Um arquivo de zona usa um formato padrão conhecido como BIND para representar registros em um formato de texto. Para obter informações sobre o formato de um arquivo de zona, consulte a entrada Zone file na Wikipedia. Informações adicionais estão disponíveis na seção 3.6.1 da RFC 1034, Domain Names—Concepts and Facilities e na seção 5 da RFC 1035, Domain Names—Implementation and Specification.

Se você quiser criar registros importando um arquivo de zona, observe o seguinte:

- O arquivo de zona deve estar em um formato compatível com a RFC.
- O nome de domínio dos registros no arquivo de zona deve corresponder ao nome da zona hospedada.
- O Route 53 oferece suporte às palavras-chave `$ORIGIN` e `$TTL`. Se o arquivo da zona incluir as palavras-chave `$GENERATE` ou `$INCLUDE`, a importação falhará e o Route 53 retornará um erro.
- Quando você importa o arquivo de zona, o Route 53 ignora o registro de SOA no arquivo de zona. O Route 53 também ignora quaisquer registros de NS que têm o mesmo nome da zona hospedada.
- Você pode importar um máximo de 1000 registros.
- Se a zona hospedada já contiver registros que aparecem no arquivo de zona, o processo de importação falhará e nenhum registro será criado.
- Recomendamos que você revise o conteúdo do arquivo de zona para confirmar se os nomes de registro incluem ou excluem um ponto final, conforme apropriado:
  - Quando o nome de um registro no arquivo de zona inclui um ponto final (`example.com.`), o processo de importação interpreta o nome como um nome de domínio totalmente qualificado e cria um registro do Route 53 com esse nome.

- Quando o nome de um registro no arquivo de zona não inclui um ponto final (`www`), o processo de importação concatena esse nome com o nome do domínio no arquivo de zona (`example.com`) e cria um registro do Route 53 com o nome concatenado (`www.example.com`).

Se o processo de exportação não adicionar um ponto final aos nomes de domínio totalmente qualificados de um registro, o processo de importação do Route 53 adicionará o nome de domínio ao nome do registro. Por exemplo, suponha que você esteja importando registros para a zona hospedada `example.com` e o nome de um registro MX no arquivo de zona seja `mail.example.com`, sem ponto final. O processo de importação do Route 53 cria um registro MX chamado `mail.example.com.example.com`.

> **Important**
>
> Para os registros CNAME, MX, PTR e SRV, este comportamento também se aplica ao nome de domínio que está incluído no valor RDATA. Por exemplo, suponha que você tem um arquivo de zona para `example.com`. Se um registro CNAME no arquivo de zona (`support`, sem um ponto final) tiver um valor RDATA de `www.example.com` (também sem um ponto final), o processo de importação criará um registro do Route 53 com o nome `support.example.com` que encaminha o tráfego para `www.example.com.example.com`. Antes de importar seu arquivo de zona, revise o valores RDATA e atualize conforme aplicável.

O Route 53 não oferece suporte à exportação de registros para um arquivo de zona.

Para criar registros importando um arquivo de zona

1. Obtenha um arquivo de zona a partir do provedor de serviços de DNS que está servindo o domínio. O processo e a terminologia variam de um provedor de serviços para outro. Consulte a interface e a documentação do provedor para obter informações sobre como exportar ou salvar seus registros em um arquivo de zona ou em um arquivo BIND

   Se o processo não for óbvio, entre em contato com o atendimento ao cliente do seu provedor de DNS atual e peça informações sobre a lista de registros ou o arquivo de zona.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.

4. Na página Hosted zones (Zonas hospedadas), crie uma nova zona hospedada:

   a. Escolha Create hosted zone (Criar zona hospedada).

   b. Digite o nome do seu domínio e, se desejar, um comentário.

   c. Escolha Criar.

5. Escolha Import zone file (Importar arquivo de zona).

6. No painel Import zone file (Importar arquivo de zona), cole o conteúdo do arquivo de zona na caixa de texto Zone file (Arquivo de zona).

7. Escolha Importar.

   > **Note**
   >
   > Dependendo do número de registros em seu arquivo de zona, talvez você precise aguardar alguns minutos para que os registros sejam criados.

8. Se você estiver usando outro serviço de DNS para o domínio (que é comum se você registrou o domínio com outro registrador), migre o serviço de DNS para o Route 53. Quando essa etapa estiver concluída, o registrador começará a identificar o Route 53 como o serviço DNS em resposta às consultas DNS do seu domínio, e as consultas começarão a ser enviadas aos servidores DNS do Route 53. (Normalmente, é necessário aguardar de um a dois dias até que as consultas de DNS comecem a ser roteadas para o Route 53. Isso ocorre porque as informações sobre o serviço de DNS anterior ficam armazenadas em cache durante este período nos resolvedores do DNS.) Para ter mais informações, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Editar registros

O procedimento a seguir explica como editar registros usando o console do Amazon Route 53. Para obter informações sobre como editar registros usando a API do Route 53, consulte ChangeResourceRecordSetsa Referência da API do Amazon Route 53.

> **Note**
>
> As alterações nos registros demoram para serem propagadas até os servidores DNS do Route 53. Atualmente, a única forma de verificar se as alterações se propagaram é usando a

ação da GetChangeAPI. As alterações geralmente são propagadas para todos os servidores de nome do Route 53 em até 60 segundos.

Para editar registros usando o console do Route 53

1. Se você não estiver editando registros de alias, vá para a etapa 2.

   Se você estiver editando registros de alias que roteiam tráfego para um Classic Load Balancer, um Application Load Balancer ou um Network Load Balancer de Elastic Load Balancing, e tiver criado a zona hospedada do Route 53 e o balanceador de carga usando contas diferentes, siga o procedimento Obter o nome do DNS para um balanceador de carga de Elastic Load Balancing para obter o nome do DNS do balanceador de carga.

   Se você estiver editando registros de alias para qualquer outro AWS recurso, vá para a etapa 2.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Na página Hosted Zones (Zonas hospedadas), selecione a linha da zona hospedada que contém os registros que deseja editar.
5. Selecione a linha do registro que você deseja editar e insira suas alterações no painel Edit record (Editar registro).
6. Insira os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica ao criar ou editar registros do Amazon Route 53.
7. Escolha Salvar alterações.
8. Se você estiver editando vários registros, repita as etapas de 5 a 7.

Excluir registros

O procedimento a seguir explica como excluir registros usando o console do Route 53.
Para obter informações sobre como excluir registros usando a API do Route 53, consulte ChangeResourceRecordSetsa Referência da API do Amazon Route 53.

> **Note**
>
> As alterações nos registros demoram para serem propagadas até os servidores DNS do Route 53. Atualmente, a única forma de verificar se as alterações se propagaram é usando a ação da GetChangeAPI. As alterações geralmente são propagadas para todos os servidores de nome do Route 53 em até 60 segundos.

Para excluir registros

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na página Zonas hospedadas, selecione a linha da zona hospedada que contém os registros que você deseja excluir.
3. Na lista de registros, selecione o registro que você quer excluir.

   Para selecionar vários registros consecutivos, selecione a primeira linha, mantenha a tecla Shift pressionada e selecione a última linha. Para selecionar vários registros não consecutivos, selecione na primeira linha, mantenha a tecla Ctrl pressionada e selecione as demais linhas.

   Você não pode excluir os registros que têm um valor de NS ou SOA para Type (Tipo).
4. Escolha Excluir.
5. Escolha Delete (Excluir) para fechar a caixa de diálogo.

Listar registros

O procedimento a seguir explica como usar o console do Amazon Route 53 para listar os registros em uma zona hospedada. Para obter informações sobre como listar registros usando a API do Route 53, consulte ListResourceRecordSetsa Referência da API do Amazon Route 53.

Para listar registros

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Zonas hospedadas, escolha o nome de uma zona hospedada.

4. Para alterar os campos da pesquisa, escolha o ícone de engrenagem no canto superior direito da tabela Records. Escolha uma destas opções:

   - Automatic

     Nesse modo, o serviço usa um filtro baseado em vários registros. Completo para menos de 2.000 e rápido para mais de 2.000 registros.

   - Full

     Nesse modo, todos os filtros de pesquisa estão disponíveis, mas a performance da pesquisa pode ser mais lenta.

   - Fast

     Nesse modo, alguns recursos avançados não estão disponíveis, mas a performance da pesquisa será mais rápida.

Para exibir somente os registros selecionados, informe os critérios de pesquisa aplicáveis acima da lista de registros. No modo automático, o comportamento da pesquisa depende de a zona hospedada conter menos ou mais de 2.000 registros:

Até 2.000 registros e modo completo

- Para exibir os registros que têm valores específicos, informe um valor na barra de pesquisa e pressione Enter. Por exemplo, para exibir os registros com um endereço IP que começa com 192.0, insira esse valor no campo Search (Pesquisar) e pressione Enter.
- Para exibir somente os registros que têm o mesmo tipo de registro DNS, selecione Record type (Tipo de registro) na lista suspensa e insira o tipo de registro.
- Para exibir somente registros de alias, selecione Aliases na lista suspensa e insira **`Yes`**.
- Para exibir somente registros ponderados, selecione Routing policy (Política de roteamento) na lista suspensa e insira **`WEIGHTED`**.

Mais de 2.000 registros e modo rápido

- Você pode pesquisar apenas nos nomes de registros, e não nos valores de registros. Também não é possível usar filtros com base no tipo de registro, no alias ou nos registros ponderados.

  Para isso, coloque o cursor na caixa de texto Filtrar, selecione Propriedades e, depois, Nome do registro.

- Em registros que possuem três rótulos (três partes separadas por pontos), quando você insere um valor no campo de pesquisa e pressiona Enter, o console do Route 53 executa automaticamente uma pesquisa com caracteres curinga no terceiro rótulo à direita no nome do registro. Por exemplo, suponha que a zona hospedada example.com contenha 100 registros denominados record1.example.com por meio de record100.example.com. (Record1 é o terceiro rótulo da direita.) Veja o que acontece quando você pesquisa os seguintes valores:
  - record1: o console do Route 53 procura por record1*.example.com, que retorna record1.example.com, record10.example.com a record19.example.com e record100.example.com.
  - record1.example.com – como no exemplo anterior, o console pesquisa record1.example.com e retorna os mesmos registros.
  - 1: o console procura por 1*.example.com e não retorna registros.
  - example: o console procura por example*.example.com e não retorna registros.
  - example.com: neste exemplo, o console não executa uma pesquisa com caractere curinga. Ele retorna todos os registros na zona hospedada.
  - Modo de pesquisa automática: quando usar esse modo de pesquisa, para pesquisar, você deverá primeiro fornecer uma propriedade, como nome do registro.

  > **Note**
  >
  > Se o terceiro rótulo da direita contiver um ou mais hifens (por exemplo, `third-label.example.com`) e, se você pesquisar a parte do terceiro rótulo imediatamente antes do hífen (`third` neste exemplo), o Route 53 não retornará registros. Em vez disso, inclua o hífen (pesquise `third-`) ou omita o caractere imediatamente antes do hífen (pesquise `third`).

- Para registros que possuem quatro ou mais rótulos, você deve especificar o nome exato do registro. Não há suporte para pesquisas curinga. Por exemplo, se a zona hospedada incluir um registro denominado label4.record1.example.com, você poderá localizar esse registro apenas se especificar label4.record1.example.com no campo de pesquisa.

Como configurar a assinatura de DNSSEC no Amazon Route 53

A assinatura de Domain Name System Security Extensions (DNSSEC) permite que os resolvedores DNS validem que uma resposta DNS veio do Amazon Route 53 e não foi adulterada. Quando

você usa a assinatura de DNSSEC, cada resposta para uma zona hospedada é assinada usando criptografia de chave pública.

Neste capítulo, explicaremos como habilitar a assinatura de DNSSEC para o Route 53, como trabalhar com chaves de assinatura de chave (KSK) e como solucionar problemas. Você pode trabalhar com a assinatura do DNSSEC AWS Management Console ou programaticamente com a API. Para obter mais informações sobre como usar a CLI ou SDKs para trabalhar com o Route 53, consulte Como configurar o Amazon Route 53.

Antes de habilitar a assinatura de DNSSEC, observe o seguinte:

- Para ajudar a evitar uma interrupção da zona e evitar que problemas com o seu domínio se tornem indisponíveis, você deve tratar e resolver rapidamente os erros de DNSSEC. É altamente recomendável que você configure um CloudWatch alarme que o alerte sempre que um `DNSSECKeySigningKeysNeedingAction` erro `DNSSECInternalFailure` ou for detectado. Para ter mais informações, consulte Monitoramento de zonas hospedadas usando a Amazon CloudWatch.
- Existem dois tipos de chaves no DNSSEC: uma chave de assinatura de chave (KSK) e uma chave de assinatura de zonas (ZSK). Na assinatura de DNSSEC do Route 53, cada KSK é baseada em uma chave assimétrica gerenciada pelo cliente no seu AWS KMS . Você é responsável pelo gerenciamento da KSK, que inclui alterná-la, se necessário. O gerenciamento de ZSK é realizado pelo Route 53.
- Quando você habilita a assinatura de DNSSEC para uma zona hospedada, o Route 53 limita o TTL a uma semana. Se você definir um TTL de mais de uma semana para registros na zona hospedada, você não receberá um erro. No entanto, o Route 53 impõe um TTL de uma semana para os registros. Registros que têm um TTL de menos de uma semana e registros em outras zonas hospedadas que não têm a assinatura de DNSSEC habilitada não são afetados.
- Quando você usa a assinatura de DNSSEC, configurações de vários fornecedores não são suportadas. Se você configurou servidores de nomes de white-label (também conhecidos como servidores de nomes personalizados ou servidores de nomes privados), certifique-se de que esses servidores de nomes sejam fornecidos por um único provedor de DNS.
- Alguns provedores de DNS não oferecem suporte a registros de Signatário de Delegação (Delegation Signer, DS) em seu DNS autoritativo. Se sua zona pai for hospedada por um provedor de DNS que não oferece suporte a consultas DS (não definindo um sinalizador AA na resposta da consulta ao DS), quando você habilitar o DNSSEC em sua zona filho, a zona filho ficará sem solução. Certifique-se de que seu provedor de DNS ofereça suporte a registros DS.

- Pode ser útil configurar permissões do IAM para permitir que outro usuário, além do proprietário da zona, adicione ou remova registros na região. Por exemplo, um proprietário de zona pode adicionar uma KSK e habilitar a assinatura, e também pode ser responsável pela rotação de chaves. No entanto, outra pessoa pode ser responsável por trabalhar com outros registros para a zona hospedada. Para ver um exemplo de política do IAM, consulte Permissões de exemplo para um proprietário de registro de domínio.

Tópicos

Como habilitar a assinatura de DNSSEC e estabelecer uma cadeia de confiança

As etapas incrementais são aplicáveis ao proprietário da zona hospedada e ao responsável por manter a zona pai. Eles podem ser a mesma pessoa, mas, se não forem, o proprietário da zona deve notificar e trabalhar com o responsável por mantê-la.

Recomendamos as etapas deste artigo para que sua zona seja assinada e incluída na cadeia de confiança. As seguintes etapas minimizam o risco de integração no DNSSEC.

> **Note**
>
> Certifique-se de ler os prerrequisitos antes de começar a usar Como configurar a assinatura de DNSSEC no Amazon Route 53.

Existem três etapas a serem seguidas para habilitar a assinatura de DNSSEC, conforme descrito nas seções abaixo:

Tópicos

Etapa 1: Preparar-se para habilitar a assinatura de DNSSEC

As etapas de preparação ajudam você a minimizar o risco de integração ao DNSSEC, monitorando a disponibilidade da zona e diminuindo os tempos de espera entre habilitar a assinatura e inserir o registro de signer da delegação (DS).

Para preparar-se para habilitar a assinatura de DNSSEC

1. Faça o monitoramento da disponibilidade da zona

   É possível fazer o monitoramento da zona para verificar a disponibilidade dos seus nomes de domínio. Isso pode ajudar você a resolver problemas que possam justificar um passo para trás depois que você habilitar a assinatura de DNSSEC. É possível fazer o monitoramento dos seus nomes de domínio com a maior parte do tráfego utilizando o registro de consultas em log. Para obter mais informações sobre como configurar o registro de consultas em log, consulte Como monitorar o Amazon Route 53.

   O monitoramento pode ser feito com o uso de um shell script ou de um serviço de terceiros. Porém, ele não deve ser o único sinal para determinar a necessidade de uma reversão. Você também pode obter feedback dos seus clientes devido à indisponibilidade de um domínio.
2. Reduza o TTL máximo da zona.

   O TTL máximo da zona é o registro de TTL mais longo que ela contém. No seguinte exemplo de zona, o TTL máximo da zona é de 1 dia (86.400 segundos).

Nome	TTL	Classe do registro	Tipo de registro	Dados do registro
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 200202240

Nome	TTL	Classe do registro	Tipo de registro	Dados do registro
				1 10800 15 604800 300
example.com.	900	IN	ns	ns1.example.com.
route53.example.com.	86400	IN	TXT	**some txt record**

Diminuir o TTL máximo da zona ajudará a reduzir o tempo de espera entre habilitar a assinatura e inserir o registro de signer de delegação (DS). Recomendamos reduzir o TTL máximo da zona para 1 hora (3.600 segundos). Isso permitirá uma reversão depois de apenas uma hora se algum resolvedor apresentar problemas com o armazenamento em cache de registros assinados.

Reversão: desfaça as alterações no TTL.

3. Diminua o campo de TTL SOA e SOA mínimo.

   O campo de SOA mínimo é o último nos dados do registro SOA. No seguinte exemplo de registro SOA, o campo mínimo tem o valor de 5 minutos (300 segundos).

Nome	TTL	Classe do registro	Tipo de registro	Dados do registro
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 200202240 1 10800 15 604800 300

O campo de TTL SOA e SOA mínimo determina por quanto tempo os resolvedores memorizam respostas negativas. Depois que você habilitar a assinatura, os servidores de nomes do Route 53 começarão a retornar registros NSEC para respostas negativas. O NSEC contém informações que os resolvedores podem usar para sintetizar uma resposta negativa. Se uma reversão for necessária porque as informações do NSEC fizeram com que um resolvedor considerasse uma resposta negativa para um nome, basta esperar o máximo do campo de TTL SOA e SOA mínimo para que o resolvedor interrompa essa suposição.

Reversão: desfaça as alterações do SOA.

4. Certifique-se de que as alterações no campo de TTL e SOA mínimo estejam efetivadas.

   Use GetChangepara garantir que suas alterações até agora tenham sido propagadas para todos os servidores DNS do Route 53.

Etapa 2: Habilitar a assinatura de DNSSEC e criar uma KSK

Você pode habilitar a assinatura do DNSSEC e criar uma chave de assinatura de chave (KSK) usando AWS CLI ou no console do Route 53.

- CLI
- Console

Quando você fornece ou cria uma chave de KMS gerenciada pelo cliente, há vários requisitos. Para ter mais informações, consulte Como trabalhar com chaves gerenciadas pelo cliente para DNSSEC.

CLI

É possível usar uma chave existente ou criar uma nova, executando um comando da AWS CLI como o seguinte e usando seus próprios valores para `hostedzone_id`, `cmk_arn`, `ksk_name` e `unique_string` (para tornar a solicitação exclusiva):

```
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
```

Para obter mais informações sobre chaves gerenciadas pelo cliente, consulte Como trabalhar com chaves gerenciadas pelo cliente para DNSSEC. Consulte também CreateKeySigningKey.

Para habilitar a assinatura do DNSSEC, execute um AWS CLI comando como o seguinte, usando seu próprio valor para: `hostedzone_id`

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

Para obter mais informações, consulte enable-hosted-zone-dnssecEnableHostedZoneDNSSEC.

Console

Para habilitar a assinatura de DNSSEC e criar uma KSK

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e depois escolha uma zona hospedada na qual você deseja habilitar a assinatura de DNSSEC.
3. Na guia DNSSEC signing (Assinatura de DNSSEC), escolha Enable DNSSEC signing (Habilitar assinatura de DNSSEC).

   > **Note**
   >
   > Se a opção nesta seção for Disable DNSSEC signing (Desabilitar a assinatura de DNSSEC), você já concluiu a primeira etapa para habilitar a assinatura de DNSSEC. Certifique-se de estabelecer, ou de que já existe, uma cadeia de confiança para a zona hospedada da DNSSEC e, em seguida, está concluído. Para ter mais informações, consulte Etapa 3: Estabelecer uma cadeia de confiança.

4. Na seção Key-signing key (KSK) creation (Criação de chaves de assinatura de chaves), selecione Create new KSK (Criar novo KSK) e, em Provide KSK name (Forneça um nome para a KSK), insira um nome para a KSK que o Route 53 criará para você. O nome só pode conter números, letras e sublinhados (_). Essa opção deve ser exclusiva.
5. Em Customer managed CMK (CMK gerenciada pelo cliente), escolha a chave gerenciada pelo cliente para o Route 53 a ser usada quando ele criar a KSK para você. Você pode usar uma chave gerenciada pelo cliente existente que se aplica à assinatura de DNSSEC ou criar uma nova chave gerenciada pelo cliente.

Quando você fornece ou cria uma chave gerenciada pelo cliente, há vários requisitos. Para ter mais informações, consulte Como trabalhar com chaves gerenciadas pelo cliente para DNSSEC.

6. Insira o alias para uma chave gerenciada pelo cliente existente. Se quiser usar uma nova chave gerenciada pelo cliente, insira um alias para a chave gerenciada pelo cliente, e o Route 53 criará uma para você.

   > **Note**
   >
   > Se você optar por fazer com que o Route 53 crie uma chave gerenciada pelo cliente, esteja ciente de que cobranças separadas se aplicam a cada chave gerenciada pelo cliente. Para mais informações, consulte Preço do serviço gerenciado pela chave da AWS.

7. Escolha Enable DNSSEC signing (Habilitar assinatura de DNSSEC).

Depois de habilitar a assinatura da zona, conclua as etapas a seguir (independentemente de ter usado o console ou a CLI):

1. Verifique se a assinatura da zona está efetiva.

   Se você usou AWS CLI, você pode usar o ID de operação da saída da `EnableHostedZoneDNSSEC()` chamada para executar get-change ou GetChangepara garantir que todos os servidores DNS do Route 53 estejam assinando respostas (status =). `INSYNC`

2. Aguarde pelo menos o TTL máximo da zona anterior.

   Aguarde até que os resolvedores liberem todos os registros não assinados de seus caches. Para isso, você deve aguardar pelo menos o TTL máximo da zona anterior. No zona `example.com` acima, o tempo de espera é de 1 dia.

3. Monitore relatórios de problemas de clientes.

   Depois de habilitar a assinatura da zona, seus clientes podem começar a perceber problemas relacionados a dispositivos de rede e a resolvedores. O período de monitoramento recomendado é de duas semanas.

   Os seguintes são exemplos de problemas com os quais você pode se deparar:

- Alguns dispositivos de rede podem limitar o tamanho das respostas de DNS a menos de 512 bytes, o que é um limite muito pequeno para algumas respostas assinadas. Esses dispositivos devem ser reconfigurados para permitirem tamanhos maiores de resposta de DNS.
- Alguns dispositivos de rede fazem uma inspeção profunda nas respostas de DNS e removem certos registros que não compreendem, como os utilizados para o DNSSEC. Esses dispositivos precisam ser reconfigurados.
- Os resolvedores de alguns clientes declaram que podem aceitar uma resposta UDP maior do que aquelas com suporte pela rede. Você pode testar a capacidade da sua rede e configurar resolvedores de acordo. Para saber mais, consulte Servidor de teste de tamanho de respostas de DNS.

Reversão: chame o DisableHostedZoneDNSSEC e, em seguida, reverta as etapas. Etapa 1: Preparar-se para habilitar a assinatura de DNSSEC

Etapa 3: Estabelecer uma cadeia de confiança

Depois de habilitar a assinatura de DNSSEC para uma zona hospedada no Route 53, estabeleça uma cadeia de confiança para que a zona hospedada conclua sua configuração de assinatura de DNSSEC. Para fazer isso, crie um registro de Signatário da Delegação (DS) na zona hospedada pai, para sua zona hospedada, usando as informações fornecidas pelo Route 53. Dependendo de onde seu domínio está registrado, você adiciona o registro à zona hospedada pai no Route 53 ou em outro registrador de domínio.

Para estabelecer uma cadeia de confiança para assinatura de DNSSEC

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e escolha uma zona hospedada para a qual você deseja estabelecer uma cadeia de confiança de DNSSEC. Você deve habilitar primeiro a assinatura de DNSSEC.
3. Na guia DNSSEC signing (Assinatura de DNSSEC), em DNSSEC signing (Assinatura de DNSSEC), escolha View information to create DS record (Exibir informações para criar registro DS).

> **Note**
>
> Se você não vir View information to create DS record (Exibir informações para criar registro DS) nesta seção, você deve habilitar a assinatura de DNSSEC antes de estabelecer a cadeia de confiança. Escolha Enable DNSSEC signing (Habilitar assinatura de DNSSEC) e conclua as etapas descritas em Etapa 2: Habilitar a assinatura de DNSSEC e criar uma KSK. Depois, retorne a essas etapas para estabelecer a cadeia de confiança.

4. Em Establish a chain of trust (Estabelecer uma cadeia de confiança), escolha Route 53 registrar (Registrador do Route 53) ou Another domain registrar (Outro registrador de domínio), dependendo de onde seu domínio está registrado.
5. Use os valores fornecidos da etapa 3 para criar um registro de DS para a zona hospedada pai no Route 53. Se o domínio não estiver hospedado no Route 53, utilize os valores fornecidos para criar um registro de DS no site do registrador de domínios.

   - Se a zona principal for um domínio gerenciado pelo Route 53, siga estas etapas:

     Certifique-se de configurar o algoritmo de assinatura correto (ECDSAP256SHA256 e tipo 13) e algoritmo de compilação (SHA-256 e tipo 2).

     Se o Route 53 for o registrador, siga este procedimento no console do Route 53:

     1. Observe os valores de Key type (Tipo de chave), Signing algorithm (Algoritmo de assinatura) e Public key (Chave pública). No painel de navegação, escolha Registered domains (Domínios registrados).
     2. Selecione um domínio e, em seguida, ao lado de DNSSEC status (Status de DNSSEC), escolha Manage keys (Gerenciar chaves).
     3. Na caixa de diálogo Manage DNSSEC keys (Gerenciar chaves de DNSSEC), escolha o Key type (Tipo de chave) apropriado e Algorithm (Algoritmo) para o Route 53 registrar (Registrador do Route 53) nos menus suspensos.
     4. Copiar a Public key (Chave pública) para o registrador do Route 53. Na caixa de diálogo Manage DNSSEC keys (Gerenciar chaves de DNSSEC), cole o valor na caixa Public key (Chave pública).
     5. Escolha Add (Adicionar).

O Route 53 adicionará o registro DS à zona pai da chave pública. Por exemplo, se o seu domínio for `example.com`, o registro DS será adicionado à zona DNS .com.

- Se a zona principal estiver hospedada no Route 53 ou se o domínio for gerenciado em outro registro, entre em contato com a zona principal ou com o proprietário do registro do domínio para seguir estas instruções:

  Para garantir que as seguintes etapas funcionem sem problemas, introduza um TTL de DS baixo na zona pai. Convém configurar o TTL de DS como 5 minutos (300 segundos) para uma recuperação mais rápida caso você precise reverter as alterações.

  - Caso sua zona pai seja administrada por outro registro, entre em contato com o registrador para introduzir o registro de DS da sua zona. Em geral, você não poderá ajustar o TTL do registro de DS.
  - Se a zona pai estiver hospedada no Route 53, entre em contato com o proprietário da zona pai para introduzir o registro de DS da sua zona.

    Forneça o `$ds_record_value` ao proprietário da zona pai. Para obtê-lo, clique em View Information to create DS record (Exibir informações para criar registro de DS) no console e copie o campo DS record (Registro de DS) ou chame a API GetDNSsec e recupere o valor do campo 'DSRecord':

    ```
    aws --region us-east-1 route53 get-dnssec
                --hosted-zone-id $hostedzone_id
    ```

    O proprietário da zona pai pode inserir o registro usando o console do Route 53 ou a CLI.

    - Para inserir o registro DS usando AWS CLI, o proprietário da zona principal cria e nomeia um arquivo JSON semelhante ao exemplo a seguir. O proprietário da zona pai pode atribuir ao arquivo um nome semelhante a `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"
                        }
                    ]
                }
            }
        ]
    }
}
```

Em seguida, execute o seguinte comando:

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- Para inserir o registro de DS usando o console:

  Abra o console do Route 53 em https://console.aws.amazon.com/route53/.

  No painel de navegação, escolha Hosted zones (Zonas hospedadas), o nome da zona hospedada e depois Create record (Criar registro). Escolha o roteamento simples para Routing policy (Política de roteamento).

  No campo Record name (Nome de registro), insira o mesmo nome que `$zone_name`, selecione DS para Record type (Tipo de registro) e insira o valor de `$ds_record_value` no campo Value (Valor) e escolha Create records (Criar registros).

Reversão: remova o DS da zona pai, aguarde o TTL do DS e depois reverta as etapas para estabelecer confiança. Se a zona pai estiver hospedada no Route 53, seu proprietário poderá alterar `Action` de `UPSERT` para `DELETE` no arquivo JSON e executar novamente o exemplo de CLI acima.

6. Aguarde até que as atualizações sejam propagadas, com base no TTL para seus registros de domínio.

   Se a zona principal estiver no serviço DNS do Route 53, o proprietário da zona principal poderá confirmar a propagação completa por meio da GetChangeAPI.

Caso contrário, você poderá sondar periodicamente a zona pai no que diz respeito ao registro DS e aguardar mais 10 minutos depois para aumentar a probabilidade de a inserção do registro de DS ser completamente propagada. Alguns registradores agendam a inserção do DS, por exemplo, uma vez ao dia.

Quando você introduz o registro de signer de delegação (DS) na zona pai, os resolvedores validados que escolheram o DS começam a validar as respostas da zona.

Para garantir que as etapas para estabelecer a confiança sigam sem problemas, faça o seguinte:

1. Localize o TTL de NS máximo.

   Existem dois conjuntos de registros de NS associados às suas zonas:

   - O registro de NS de delegação, ou seja, o registro de NS da sua zona mantida pela zona pai. Você pode encontrá-lo executando os seguintes comandos Unix (se sua zona for example.com, a zona pai será com):

     ```
     dig -t NS com
     ```

     Escolha um dos registros de NS e execute o seguinte:

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     Por exemplo:

     ```
     dig @b.gtld-servers.net. -t NS example.com
     ```

   - O registro de NS na zona, ou seja, o registro de NS na sua zona. Você pode localizá-lo executando o seguinte comando Unix:

     ```
     dig @one of the NS records of your zone -t NS example.com
     ```

     Por exemplo:

     ```
     dig @ns-0000.awsdns-00.co.uk. -t NS example.com
     ```

     Observe o TTL máximo de ambas as zonas.

2. Aguarde o TTL de NS máximo.

Antes da inserção do DS, os resolvedores recebem uma resposta assinada, mas não validam a assinatura. Quando o registro de DS for inserido, os resolvedores apenas o verão quando o registro de NS da zona expirar. Quando os resolvedores voltarem a buscar o registro de NS, o registro de DS também será retornado.

Se o seu cliente estiver executando um resolvedor em um host com um relógio fora de sincronia, verifique se esse relógio está dentro de 1 hora após a hora correta.

Depois que você concluir essa etapa, todos os resolvedores com reconhecimento de DNSSEC validarão sua zona.

3. Observe a resolução de nomes.

   Você deve observar que não existem problemas com resolvedores validando sua zona. Não deixe de considerar o tempo necessário para os seus clientes informarem problemas para você.

   Convém fazer um monitoramento por até 2 semanas.

4. (Opcional) Prolongue os TTLs de DS e NS.

   Se estiver satisfeito com a configuração, você poderá salvar as alterações de TTL e SOA feitas. O Route 53 limita o TTL a 1 semana para zonas assinadas. Para ter mais informações, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

   Se você puder alterar o TTL de DS, recomendamos defini-lo como 1 hora.

Como desabilitar a assinatura de DNSSEC

As etapas para desabilitar a assinatura de DNSSEC no Route 53 variam, dependendo da cadeia de confiança da qual sua zona hospedada faz parte.

Por exemplo, sua zona hospedada pode ter uma zona pai que tenha um registro de Signatário da Delegação (DS), como parte de uma cadeia de confiança. Sua zona hospedada também pode ser uma zona pai para zonas filho que habilitaram a assinatura de DNSSEC, que é outra parte da cadeia de confiança. Investigue e determine toda a cadeia de confiança para sua zona hospedada antes de executar as etapas para desabilitar a assinatura de DNSSEC.

A cadeia de confiança para sua zona hospedada que habilita a assinatura de DNSSEC deve ser cuidadosamente desfeita à medida que você desabilita a assinatura. Para remover sua zona hospedada da cadeia de confiança, você remove todos os registros DS que estão em vigor para a

cadeia de confiança que inclui essa zona hospedada. Isso significa que você deve fazer o seguinte, na ordem:

1. Remover todos os registros DS que esta zona hospedada tem para zonas filho que fazem parte de uma cadeia de confiança.
2. Remova o registro de DS da zona pai. Ignore essa etapa se tiver uma ilha de confiança (não há registros de DS na zona pai e não há registros de DS para zonas filho nessa zona).
3. Se você não conseguir remover registros DS, para remover a zona da cadeia de confiança, remova os registros NS da zona pai. Para ter mais informações, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

As seguintes etapas incrementais permitem monitorar a eficácia das etapas individuais para evitar problemas de disponibilidade de DNS na sua zona.

Para desabilitar a assinatura de DNSSEC

1. Faça o monitoramento da disponibilidade da zona

   É possível fazer o monitoramento da zona para verificar a disponibilidade dos seus nomes de domínio. Isso pode ajudar você a resolver problemas que possam justificar um passo para trás depois que você habilitar a assinatura de DNSSEC. É possível fazer o monitoramento dos seus nomes de domínio com a maior parte do tráfego utilizando o registro de consultas em log. Para obter mais informações sobre como configurar o registro de consultas em log, consulte Como monitorar o Amazon Route 53.

   O monitoramento pode ser feito com o uso de um shell script ou de um serviço pago. Porém, ele não deve ser o único sinal para determinar a necessidade de uma reversão. Você também pode obter feedback dos seus clientes devido à indisponibilidade de um domínio.

2. Localize o TTL de DS atual.

   Você pode localizar o TTL de DS executando o seguinte comando Unix:

   ```
   dig -t DS example.com example.com
   ```

3. Localize o TTL de NS máximo.

   Existem dois conjuntos de registros de NS associados às suas zonas:

- O registro de NS de delegação, ou seja, o registro de NS da sua zona mantida pela zona pai. Você pode alterar isso executando os seguintes comandos Unix:

  Primeiro, localize o NS da sua zona pai (se sua zona for exemplo.com, a zona pai será com):

  ```
  dig -t NS com
  ```

  Escolha um dos registros de NS e execute o seguinte:

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  Por exemplo:

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- O registro de NS na zona, ou seja, o registro de NS na sua zona. Você pode localizá-lo executando o seguinte comando Unix:

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  Por exemplo:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  Observe o TTL máximo de ambas as zonas.

4. Remova o registro de DS da zona pai.

   Entre em contato com o proprietário da zona pai para remover o registro de DS.

   Reversão: reinsira registro do DS, confirme que a inserção do DS foi efetivada e aguarde o TTL máximo do NS (não do DS) antes que todos os resolvers comecem a validar novamente.

5. Confirme se a remoção do DS foi efetivada.

   Se a zona principal estiver no serviço DNS do Route 53, o proprietário da zona principal poderá confirmar a propagação completa por meio da GetChangeAPI.

   Caso contrário, você poderá sondar periodicamente a zona pai no que diz respeito ao registro DS e aguardar mais 10 minutos depois para aumentar a probabilidade de a remoção do registro de DS ser completamente propagada. Alguns registradores agendam a remoção do DS, por exemplo, uma vez ao dia.

6. Aguarde o TTL de DS.

Aguarde até que todos os resolvedores tenham expirado o registro de DS de seus caches.

7. Desabilite a assinatura de DNSSEC e desative a chave de assinatura de chaves (KSK).

   - CLI
   - Console

   CLI

   Chame o DisableHostedZoneDNSSEC e DeactivateKeySigningKeyas APIs.

   Por exemplo: .

```
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

   Para desabilitar a assinatura de DNSSEC

   1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
   2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e escolha uma zona hospedada na qual você deseja desabilitar a assinatura de DNSSEC.
   3. Na guia DNSSEC signing (Assinatura do DNSSEC), escolha Disable DNSSEC signing (Desabilitar assinatura de DNSSEC).
   4. Na página Disable DNSSEC signing (Desabilitar a assinatura de DNSSEC), escolha uma das opções a seguir, dependendo do cenário da zona para a qual você está desabilitando a assinatura de DNSSEC.
      - Parent zone only (Somente zona pai): esta zona tem uma zona pai com um registro DS. Nesse cenário, você deve remover o registro DS da zona pai.

- Child zones only (Somente zonas filho): esta zona tem um registro DS para uma cadeia de confiança com uma ou mais zonas filho. Nesse cenário, você deve remover registros DS da zona.
- Parent and child zones (Zonas pai e filho): esta zona tem um registro DS para uma cadeia de confiança com uma ou mais zonas filho e uma zona pai com um registro DS. Para esse cenário, faça o seguinte na ordem:

  a. Remova os registros DS da zona.

  b. Remova o registro DS da zona pai.

  Se tiver uma ilha de confiança, ignore essa etapa.

5. Determine qual é o TTL de cada registro de DS que você remover na Etapa 4 e verifique se o período de TTL mais longo expirou.
6. Marque a caixa de seleção para confirmar que você seguiu as etapas na ordem.
7. Digite disable (desabilitar) no campo, conforme mostrado, e escolha Disable (Desabilitar).

Para desativar a chave de assinatura de chaves (KSK)

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e escolha uma zona hospedada cuja chave de assinatura de chaves (KSK) você queira desativar.
3. Na seção Key-signing keys (KSKs) Chaves de assinatura de chaves), escolha a KSK que você deseja desativar e, em Actions (Ações), escolha Edit KSK (Editar KSK), defina KSK Status (Status da KSK) como Inactive (Inativa) e depois escolha Save KSK (Salvar KSK).

Reversão: APIs de chamadas ActivateKeySigningKeye EnableHostedZoneDNSSEC.

Por exemplo: .

```
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. Confirme que a ação de desabilitar a assinatura da zona foi efetivada.

   Use o ID da `EnableHostedZoneDNSSEC()` chamada a ser executada GetChangepara garantir que todos os servidores DNS do Route 53 tenham parado de assinar respostas (status `=INSYNC`).

9. Observe a resolução de nomes.

   Você deve observar que não há problemas resultando na validação da sua zona pelos resolvedores. Aguarde de uma a duas semanas para também considerar o tempo necessário para os seus clientes informarem problemas para você.

10. (Opcional) Limpe.

    Se você não reativar a assinatura, poderá limpar os KSKs DeleteKeySigningKeye excluir a chave gerenciada pelo cliente correspondente para economizar custos.

Como trabalhar com chaves gerenciadas pelo cliente para DNSSEC

Quando você habilita a assinatura DNSSEC no Amazon Route 53, o Route 53 cria uma chave de assinatura de chave (KSK). Para criar um KSK, o Route 53 deve usar uma chave gerenciada pelo cliente AWS Key Management Service que ofereça suporte ao DNSSEC. Esta seção descreve os detalhes e os requisitos para a chave gerenciada pelo cliente que são úteis conhecer ao trabalhar com o DNSSEC.

Lembre-se do seguinte ao trabalhar com chaves gerenciadas pelo cliente para DNSSEC:

- A chave gerenciada pelo cliente que você usa com a assinatura de DNSSEC deve estar na região Leste dos EUA (Norte da Virgínia).
- A chave gerenciada pelo cliente deve ser uma chave assimétrica gerenciada pelo cliente com uma especificação principal ECC_NIST_P256. Essas chaves gerenciadas pelo cliente são usadas somente para assinatura e verificação. Para obter ajuda na criação de uma chave assimétrica gerenciada pelo cliente, consulte Criação de chaves assimétricas gerenciadas pelo cliente no Guia do desenvolvedor. AWS Key Management Service Para obter ajuda para encontrar a configuração criptográfica de uma chave gerenciada pelo cliente existente, consulte Visualização da configuração criptográfica das chaves gerenciadas pelo cliente no Guia do AWS Key Management Service desenvolvedor.

- Se você criar uma chave gerenciada pelo cliente para usar com o DNSSEC no Route 53, deverá incluir instruções de política de chave específicas que concedam ao Route 53 as permissões necessárias. O Route 53 deve ser capaz de acessar sua chave gerenciada pelo cliente para que ele possa criar uma KSK para você. Para ter mais informações, consulte Permissões de chave gerenciada pelo cliente do Route 53 necessárias para assinatura DNSSEC.
- O Route 53 pode criar uma chave gerenciada pelo cliente para você usar com AWS KMS a assinatura do DNSSEC sem permissões adicionais AWS KMS . No entanto, você deve ter permissões específicas se quiser editar a chave depois que ela for criada. As permissões específicas que você deve ter são as seguintes: `kms:UpdateKeyDescription`, `kms:UpdateAlias` e `kms:PutKeyPolicy`.
- Esteja ciente de que cobranças separadas se aplicam a cada chave gerenciada pelo cliente que você possui, quer você crie a chave gerenciada pelo cliente ou o Route 53 a crie para você. Para obter mais informações, consulte Preço do AWS Key Management Service.

Como trabalhar com chaves de assinatura de chave (KSK)

Quando você habilita a assinatura de DNSSEC, o Route 53 cria uma chave de assinatura de chave (KSK) para você. É possível ter até duas KSKs por zona hospedada no Route 53. Depois de habilitar a assinatura de DNSSEC, você pode adicionar, remover ou editar suas KSKs.

Observe o seguinte ao trabalhar com suas KSKs:

- Antes de excluir uma KSK, você deve editar a KSK para definir seu status como Inactive (Inativo).
- Quando a assinatura de DNSSEC estiver habilitada para uma zona hospedada, o Route 53 limitará o TTL a uma semana. Se você definir um TTL para registros na zona hospedada como mais de uma semana, não receberá um erro, mas o Route 53 vai impor um TTL de uma semana.
- Para ajudar a evitar uma interrupção da zona e evitar que problemas com o seu domínio se tornem indisponíveis, você deve tratar e resolver rapidamente os erros de DNSSEC. É altamente recomendável que você configure um CloudWatch alarme que o alerte sempre que um `DNSSECKeySigningKeysNeedingAction` erro `DNSSECInternalFailure` ou for detectado. Para ter mais informações, consulte Monitoramento de zonas hospedadas usando a Amazon CloudWatch.
- As operações KSK descritas nesta seção permitem que você alterne as KSK da sua zona. Para obter mais informações e um step-by-step exemplo, consulte DNSSEC Key Rotation na postagem do blog Configurando a assinatura e validação do DNSSEC com o Amazon Route 53.

Para trabalhar com KSKs no AWS Management Console, siga as orientações nas seções a seguir.

Adicionar uma chave de assinatura de chave (KSK)

Quando você habilita a assinatura de DNSSEC, o Route 53 cria uma assinatura de chave (KSK) para você. Você também pode adicionar KSKs separadamente. É possível ter até duas KSKs por zona hospedada no Route 53.

Ao criar uma KSK, você deve fornecer ou solicitar o Route 53 para criar uma chave gerenciada pelo cliente para usar com a KSK. Quando você fornece ou cria uma chave gerenciada pelo cliente, há vários requisitos. Para ter mais informações, consulte Como trabalhar com chaves gerenciadas pelo cliente para DNSSEC.

Siga estas etapas para adicionar uma KSK no AWS Management Console.

Como adicionar uma KSK

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e, em seguida, escolha uma zona hospedada.
3. Na guia DNSSEC signing (Assinatura do DNSSEC), em Key-signing keys (KSKs) (Chaves de assinatura de chave [KSK]), escolha Switch to advanced view (Alternar para exibição avançada) e, em seguida, em Actions (Ações), escolha Add KSK (Adicionar KSK).
4. Em KSK, insira um nome para a KSK que o Route 53 criará para você. O nome só pode conter números, letras e sublinhados (_). Essa opção deve ser exclusiva.
5. Insira o alias para uma chave gerenciada pelo cliente que se aplique à assinatura de DNSSEC ou insira um alias para uma nova chave gerenciada pelo cliente que o Route 53 criará para você.

   > **Note**
   >
   > Se você optar por fazer com que o Route 53 crie uma chave gerenciada pelo cliente, esteja ciente de que cobranças separadas se aplicam a cada chave gerenciada pelo cliente. Para obter mais informações, consulte Preços do AWS Key Management Service.

6. Escolha Create KSK (Criar KSK).

Edite uma chave de assinatura de chave (KSK)

Você pode editar o status de uma KSK para ser Active (Ativo) ou Inactive (Inativo). Quando uma KSK está ativa, o Route 53 usa essa KSK para assinatura de DNSSEC. Antes de excluir uma KSK, você deve editar a KSK para definir seu status como Inactive (Inativo).

Siga estas etapas para editar uma KSK no AWS Management Console.

Para editar uma KSK

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e, em seguida, escolha uma zona hospedada.
3. Na guia DNSSEC signing (Assinatura de DNSSEC), em Key-signing keys (KSKs) (Chaves de assinatura de chaves), escolha Switch to advanced view (Alternar para exibição avançada) e, em seguida, em Actions (Ações), escolha Edit KSK (Editar KSK).
4. Faça as atualizações desejadas na KSK e escolha Save (Salvar).

Excluir uma chave de assinatura de chave (KSK)

Antes de excluir uma KSK, você deve editar a KSK para definir seu status como Inactive (Inativo).

Um dos motivos pelos quais você pode excluir uma KSK é como parte da rotação de chaves de rotina. É uma prática recomendada rotacionar chaves criptográficas periodicamente. Sua organização pode ter orientação padrão para a frequência de rotação das chaves.

Siga estas etapas para excluir uma KSK no AWS Management Console.

Para excluir uma KSK

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Hosted zones (Zonas hospedadas) e, em seguida, escolha uma zona hospedada.
3. Na guia DNSSEC signing (Assinatura de DNSSEC), em Key-signing keys (KSKs) (Chaves de assinatura de chave [KSK]), escolha Switch to advanced view (Alternar para exibição avançada) e, em Actions (Ações), escolha Delete KSK (Excluir KSK).

4. Siga as orientações para confirmar a exclusão da KSK.

Gerenciamento de chaves do KMS e de ZSK no Route 53

Esta seção descreve a prática atual que o Route 53 usa em suas zonas habilitadas para assinatura de DNSSEC.

> **Note**
>
> O Route 53 usa a regra a seguir, que pode ser alterada. Alterações futuras não reduzirão o procedimento de segurança de sua zona ou do Route 53.

Como o Route 53 usa o AWS KMS associado ao seu KSK

No DNSSEC, utiliza-se a KSK para gerar a assinatura de registro do recurso (RRSIG) para o conjunto de registros do recurso da DNSKEY. Todas as KSKs `ACTIVE` são usadas na geração de RRSIG. O Route 53 gera um RRSIG chamando a `Sign` AWS KMS API na chave KMS associada. Para obter mais informações, consulte Sign (Assinar) no Guia de referência da API do AWS KMS . Esses RSIGs não são considerados para o limite do conjunto de registros do recurso da zona.

O RRSIG tem validade. Para evitar que os RRSIGs percam a validade, os RRSIGs são atualizados regularmente, regenerando-os a cada período de um a sete dias.

Os RRSIGs também são atualizados toda vez que você chama qualquer uma dessas APIs:

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Toda vez que o Route 53 realiza uma atualização, geramos 15 RRSIGs para cobrir os próximos dias, caso a chave do KMS associada fique inacessível. Para uma estimativa de custo da chave do KMS, considere uma atualização regular uma vez por dia. Uma chave do KMS pode ficar inacessível por alterações inesperadas na política de chaves do KMS. A chave do KMS inacessível definirá o status da KSK associada como `ACTION_NEEDED`. É altamente recomendável que você monitore essa condição configurando um CloudWatch alarme sempre

que um `DNSSECKeySigningKeysNeedingAction` erro for detectado, pois a validação dos resolvedores iniciará pesquisas com falha após a expiração do último RRSIG. Para ter mais informações, consulte Monitoramento de zonas hospedadas usando a Amazon CloudWatch.

Como o Route 53 gerencia a ZSK da zona

Cada nova zona hospedada com assinatura DNSSEC ativada terá uma chave de assinatura de zona (ZSK) `ACTIVE`. A ZSK é gerada separadamente para cada zona hospedada e pertence ao Route 53. O algoritmo da chave atual é ECDSAP256SHA256.

Começaremos a executar a alternância regular da ZSK na zona no período de 7 a 30 dias após o início da assinatura. Atualmente, o Route 53 usa o método de sobreposição de chave pré-publicação. Para obter mais informações, consulte Pre-Publish Zone Signing Key Rollover (Sobreposição de chave de assinatura de zona pré-publicação). Esse método introduzirá outro ZSK à zona. A alternância será repetida a cada período de 7 a 30 dias.

O Route 53 suspenderá a alternância da ZSK se alguma KSK da zona estiver com o status `ACTION_NEEDED`, pois o Route 53 não poderá gerar novamente os RRSIGs para conjuntos de registros do recurso da DNSKEY para contabilizar as alterações na ZSK da zona. A alternância da ZSK será retomada automaticamente após a condição ser apagada.

Provas do DNSSEC de inexistência no Route 53

> **Note**
>
> O Route 53 usa a regra a seguir, que pode ser alterada. Alterações futuras não reduzirão o procedimento de segurança de sua zona ou do Route 53.

Há três tipos de prova de inexistência no DNSSEC:

- Prova de inexistência de um registro correspondente ao nome da consulta.
- Prova de inexistência de um tipo correspondente ao tipo da consulta.
- Prova de existência de um registro curinga usado para gerar o registro em resposta.

O Route 53 implementa a prova de inexistência de um registro correspondente ao nome da consulta usando o método BL. Para obter mais informações, consulte BL. É um método que produz uma representação compacta da prova e evita a verificação de zona.

Nos casos em que há um registro correspondente ao nome da consulta, mas não ao tipo de consulta (como consultar web.example.com/AAAA, mas há apenas web.example.com/A presente), retornamos um registro NSEC (próximo registro seguro) mínimo contendo todos os tipos de registro do recurso compatíveis.

Quando o Route 53 sintetizar uma resposta de um registro coringa, a resposta não será acompanhada com um próximo registro seguro ou um registro NSEC para o coringa. Esse registro NSEC é usado em algumas implementações, geralmente naquelas que executam assinatura offline, para evitar que as assinaturas de registro do recurso (RRSIG) na resposta sejam reutilizadas para falsificar uma resposta diferente. O Route 53 usa assinatura online para registros não DNSKEY a fim de gerar RRSIGs específicos para a resposta que não podem ser reutilizados para uma resposta diferente.

Como solucionar problemas de assinatura de DNSSEC

As informações nesta seção podem ajudar você a resolver problemas com a assinatura de DNSSEC, inclusive com a habilitação, desabilitação e suas chaves de assinatura de chave (KSKs).

Como habilitar DNSSEC

Certifique-se de ler os prerrequisitos em Como configurar a assinatura de DNSSEC no Amazon Route 53 antes de começar a habilitar assinatura DNSSEC.

Como desabilitar DNSSEC

Para desabilitar o DNSSEC com segurança, o Route 53 verificará se a zona de destino está na cadeia de confiança. Ele verifica se o pai da zona de destino tem algum registro NS da zona de destino e registros DS da zona de destino. Se a zona de destino não puder ser resolvida publicamente, por exemplo, obtendo uma resposta SERVFAIL ao consultar NS e DS, o Route 53 não poderá determinar se é seguro desabilitar o DNSSEC. Você pode entrar em contato com sua zona pai para corrigir esses problemas e tentar desabilitar o DNSSEC novamente mais tarde.

O status da KSK é Action needed (Ação necessária)

Uma KSK pode mudar seu status para Ação necessária (ou `ACTION_NEEDED` em um KeySigningKeystatus) quando o Route 53 DNSSEC perde acesso a uma correspondente AWS KMS key (devido a uma alteração nas permissões ou AWS KMS key exclusão).

Se o status de uma KSK for Action needed (Ação necessária), significa que, eventualmente, ele causará uma interrupção de zona para clientes que usam resolvedores de validação de DNSSEC,

e você deverá agir rapidamente para evitar que uma zona de produção se torne incapaz de ser resolvida.

Para corrigir o problema, certifique-se de que a chave gerenciada pelo cliente na qual a KSK se baseia está habilitada e tem as permissões corretas. Para mais informações sobre as permissões necessárias, consulte Permissões de chave gerenciada pelo cliente do Route 53 necessárias para assinatura DNSSEC.

Depois de corrigir o KSK, ative-o novamente usando o console ou o AWS CLI, conforme descrito emEtapa 2: Habilitar a assinatura de DNSSEC e criar uma KSK.

Para evitar esse problema no futuro, considere adicionar uma Amazon CloudWatch métrica para rastrear o estado do KSK, conforme sugerido emComo configurar a assinatura de DNSSEC no Amazon Route 53.

O status da KSK é Internal failure (Falha interna)

Quando uma KSK tem um status de falha interna (ou `INTERNAL_FAILURE` em um KeySigningKeystatus), você não pode trabalhar com nenhuma outra entidade do DNSSEC até que o problema seja resolvido. Você deve tomar medidas antes de poder trabalhar com a assinatura de DNSSEC, inclusive trabalhar com esta KSK ou com outra KSK.

Para corrigir o problema, tente novamente habilitar ou desabilitar a KSK.

Para corrigir o problema ao trabalhar com as APIs, tente ativar a assinatura (EnableHostedZoneDNSSEC) ou desativar a assinatura (DNSSEC). DisableHostedZone

É importante que você corrija os problemas de Internal failure (Falha interna) prontamente. Você não pode fazer outras alterações na zona hospedada até que você corrija o problema, exceto as operações para corrigir a Internal failure (Falha interna).

Usando AWS Cloud Map para criar registros e verificações de saúde

Para encaminhar tráfego da Internet ou tráfego dentro de uma Amazon VPC para componentes de aplicações ou microsserviços, é possível usar o AWS Cloud Map para criar registros automaticamente e, opcionalmente, criar verificações de integridade. Para mais informações, consulte o Guia do desenvolvedor do AWS Cloud Map.

Restrições e comportamentos de DNS

As mensagens de DNS estão sujeitas a fatores que afetam a maneira como você cria e usa zonas hospedadas e registros. Esta seção explica esses fatores.

Tamanho máximo da resposta

Para fins de conformidade com os padrões de DNS, as respostas enviadas por UDP são limitadas a 512 bytes de tamanho. As respostas que excedem 512 bytes são truncadas, e o resolvedor precisa enviar a solicitação novamente por TCP. Se o Resolver oferecer suporte para EDNS0 (conforme definido na RFC 2671) e anunciar a opção EDNS0 ao Amazon Route 53, o Route 53 permitirá respostas de até 4096 bytes por UDP, sem truncamento.

Processamento da seção autorizada

Para consultas bem-sucedidas, o Route 53 anexa registros do servidor de nomes (NS) da zona hospedada relevante à seção Authority (Autoridade) da resposta de DNS. Para nomes não encontrados (respostas NXDOMAIN), o Route 53 acrescenta o registro de início de autoridade (SOA) (conforme definido na RFC 1035) da zona hospedada relevante à seção Authority (Autoridade) da resposta DNS.

Processamento da seção adicional

O Route 53 anexa registros à seção Additional (Adicional). Se os registros forem conhecidos e apropriados, o serviço anexará registros A ou AAAA para qualquer destino de um registro MX, CNAME, NS ou SRV citado na seção de resposta. Para obter mais informações sobre esses tipos de registro de DNS, consulte Tipos de registro de DNS com suporte.

Usar o fluxo de tráfego para rotear o tráfego de DNS

O fluxo de tráfego simplifica muito o processo de criação e manutenção de registros em configurações grandes e complexas.

Gerenciar registros relacionados em uma zona hospedada pode ser desafiador nas seguintes circunstâncias:

- Você tem muitos recursos que executam a mesma operação, como servidores web que enviam tráfego para o mesmo domínio.
- Você deseja criar uma árvore complexa de registros usando registros de alias e uma combinação de políticas de roteamento do Route 53, como latência, failover e ponderado.

Vantagens do fluxo de tráfego

Para facilitar o rastreamento dos registros e seus relacionamentos, o fluxo de tráfego simplifica a criação de registros DNS com os seguintes recursos:

Editor visual

O editor visual de fluxo de tráfego permite criar árvores complexas de registros e ver as relações entre os registros. Por exemplo, é possível criar uma configuração na qual os registros de alias de latência referenciem registros ponderados e os registros ponderados referenciem recursos em várias Regiões da AWS. Cada configuração é conhecida como uma política de tráfego. É possível criar quantas políticas de tráfego quiser sem custos.

Versionamento

É possível criar várias versões de uma política de tráfego para que você não precise começar tudo de novo quando sua configuração for alterada. As versões antigas continuam a existir até que você as exclua; há um limite padrão de 1000 versões por política de tráfego. Opcionalmente, é possível fornecer uma descrição a cada versão.

Criação e atualização automática de registros

Uma política de tráfego pode representar dezenas ou até mesmo centenas de registros. O fluxo de tráfego permite criar todos esses registros automaticamente criando um registro de política de tráfego. Especifique a zona hospedada e o nome do registro na raiz da árvore, como exemplo.com ou www.exemplo.com, e o Route 53 criará automaticamente todos os outros

registros na árvore. O registro raiz, o registro da política de tráfego, é exibido na lista de registros da sua zona hospedada; todos os outros registros são ocultos.

Ao criar uma nova versão de uma política de tráfego, é possível atualizar seletivamente registos de política de tráfego criados usando a versão de política de tráfego anterior. Ao atualizar um registo de política de tráfego, o Route 53 atualiza automaticamente todos os outros registos na árvore. Também é possível reverter rapidamente as alterações atualizando novamente um registro de política de tráfego para usar uma versão anterior de uma política de tráfego.

> **Note**
>
> É possível usar o fluxo de tráfego para criar registros somente em zonas hospedadas públicas.

Política de roteamento de geoproximidade

Ao usar o fluxo de tráfego, você pode entender de forma mais intuitiva como o tráfego é roteado para cada um dos seus endpoints globais usando o mapa de geoproximidade na tela visual do fluxo de tráfego. Para ter mais informações, consulte Roteamento por geoproximidade.

Reutilizar para vários registros em diferentes zonas hospedadas

É possível usar uma política de tráfego para criar registros automaticamente em várias zonas hospedadas públicas. Por exemplo, se você estiver usando os mesmos servidores web para vários nomes de domínio, será possível usar a mesma política de tráfego para criar registros de política de tráfego nas zonas hospedadas para exemplo.com, exemplo.org e exemplo.net.

Quando um cliente envia uma consulta para o nome do registro raiz, como exemplo.com ou www.exemplo.com, o Route 53 responde à consulta com base na configuração da política de tráfego usada para criar o registro de política de tráfego correspondente.

Há uma cobrança mensal para cada registro de política de tráfego. Para obter mais informações, consulte a seção "Fluxo de tráfego" da Definição de preço do Amazon Route 53.

Para minimizar essas cobranças, é possível criar um ou mais registros de alias em uma zona hospedada que fazem referência a um registro de política de tráfego nessa zona hospedada. Por exemplo, é possível criar um registro de política de tráfego para exemplo.com e criar um registro de alias para www.exemplo.com que faça referência ao registro de política de tráfego.

Criar e gerenciar políticas de tráfego

Tópicos

Criar uma política de tráfego

Para criar uma política de tráfego, execute o procedimento a seguir.

Para criar uma política de tráfego

1. Elabore a sua configuração. Para obter informações sobre como as configurações complexas de roteamento de DNS funcionam, consulte Configurar failover de DNS Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.
2. Com base no projeto da configuração, crie as verificações de integridade que deseja usar para seus endpoints.
3. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
4. No painel de navegação, selecione Políticas de tráfego.
5. Selecione Criar política de tráfego.
6. Na página Política de nome, especifique os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica quando cria uma política de tráfego.
7. Escolha Próximo.
8. Na página Create traffic policy (Criar política de tráfego) policy name (nome da política) v1, especifique os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica quando cria uma política de tráfego.

Você pode excluir regras, endpoints e ramificações de uma política de tráfego das seguintes formas:

- Para excluir uma regra ou endpoint, clique no x no canto superior direito da caixa.

  > **Important**
  >
  > Se você excluir uma regra que tem regras filho e endpoints, o Amazon Route 53 também excluirá todos os filhos.

- Se você conectar duas regras à mesma regra filho ou endpoint e quiser excluir uma das conexões, posicione o cursor na conexão que deseja excluir e clique no x da conexão.

9. Selecione Criar política de tráfego.
10. Opcional: na página Create policy records with traffic policy (Criar registros de política com política de tráfego), use a nova política de tráfego para criar um ou mais registros de política em uma zona hospedada. Para ter mais informações, consulte Valores que você especifica quando cria ou atualiza um registro de política. Você também pode criar registros de política mais tarde, na mesma zona hospedada ou em zonas hospedadas adicionais.

    Se você não quiser criar registros de política agora, escolha Ignorar esta etapa e o console exibirá a lista de políticas de tráfego e registros de políticas que você criou usando a AWS conta atual.
11. Se você especificou configurações para os registros de política na etapa anterior, escolha Criar registro de política.

Valores que você especifica quando cria uma política de tráfego

Quando cria uma política de tráfego, você especifica os valores a seguir.

-
-
-
-
-
-

•

Nome da política

Digite um nome que descreva a política de tráfego. Esse valor é exibido na lista de políticas de tráfego no console. Você não poderá alterar o nome de uma política de tráfego depois de criá-la.

Version (Versão)

Esse valor é atribuído automaticamente pelo Amazon Route 53 quando você cria uma política de tráfego ou uma nova versão de uma política existente.

Descrição da versão

Digite uma descrição que se aplica a esta versão da política de tráfego. Esse valor é exibido na lista de versões de política de tráfego no console.

Tipo de DNS

Escolha o tipo de DNS que você deseja que o Amazon Route 53 atribua a todos os registros quando você cria um registro de política usando essa versão de política de tráfego. Para obter uma lista de tipos com suporte, consulte Tipos de registro de DNS com suporte.

> **Important**
>
> Se você estiver criando uma nova versão de uma política de tráfego existente, pode alterar o tipo de DNS. No entanto, você não pode editar um registro de política e escolher uma versão da política de tráfego que tenha um tipo de DNS diferente da versão da política de tráfego usada para criar o registro de política. Por exemplo, se você criou um registro de política usando uma versão de política de tráfego que tenha um tipo de DNS A, você não pode editar o registro de política e escolher versão de política de tráfego que tenha qualquer outro valor para o tipo de DNS.

Se você quiser rotear o tráfego para os seguintes AWS recursos, escolha o valor aplicável:

- CloudFront distribuição — Escolha A: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6.

- Application Load Balancer de ELB: escolha AA: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6.
- Classic Load Balancer de ELB: escolha A: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6.
- Network Load Balancer de ELB: escolha AA: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6.
- Ambiente do Elastic Beanstalk: escolha A: endereço IP no formato IPv4.
- Amazon S3 bucket configured as a website endpoint (Bucket do Amazon S3 configurado como endpoint do site): escolha A: IP address in IPv4 format (A: endereço IP no formato IPv4).

Conecte-se a

Escolha o endpoint ou regra aplicável de acordo com o projeto da sua configuração.

Regra de failover

Escolha essa opção quando quiser configurar o failover ativo-passivo, em que um recurso leva todo o tráfego quando disponível e o outro recurso leva todo o tráfego quando o primeiro recurso não está disponível.

Para ter mais informações, consulte Failover ativo/passivo.

Regra de localização geográfica

Escolha esta opção quando quiser que o Amazon Route 53 responda às consultas de DNS com base na localização de seus usuários.

Para ter mais informações, consulte Roteamento de localização geográfica.

Quando você escolhe a Geolocation rule, você também escolhe o país ou o estado nos Estados Unidos do qual as solicitações se originam.

Regra de latência

Escolha esta opção quando tiver recursos em vários datacenters do Amazon EC2 que executam a mesma função e você desejar que o Route 53 responda às consultas de DNS com os recursos que fornecem a melhor latência.

Quando você escolhe Regra de latência, também escolhe uma Região da AWS.

Para ter mais informações, consulte Roteamento baseado em latência.

Regra de geoproximity

Escolha essa opção quando desejar que o Route 53 responda a consultas ao DNS com base na localização dos recursos e, opcionalmente, em um desvio especificado por você. O desvio permite que você envie mais tráfego para um recurso ou mais tráfego de saída de um recurso.

Ao escolher a Geoproximity rule, insira os seguintes valores:

Local do endpoint

Escolha o valor aplicável:

- Personalizado (inserir coordenadas) — Se seu endpoint não for um AWS recurso, escolha Personalizado (inserir coordenadas).
- Um Região da AWS — Se o seu endpoint for um AWS recurso, escolha aquele em Região da AWS que você criou o recurso.
- Uma zona AWS local — Se seu endpoint for um AWS recurso, escolha a zona AWS local na qual você criou o recurso.

Se você usa Zonas AWS Locais, você deve primeiro habilitá-las. Para mais informações, consulte Getting started with Local Zones no AWS Local Zones User Guide.

Para ver as zonas locais disponíveis, consulte Localizações das zonas locais da AWS.

Para saber mais sobre a diferença entre Zonas Locais Regiões da AWS e Zonas Locais, consulte Regiões e Zonas no Guia do Usuário do Amazon EC2.

> **Important**
>
> Uma única política de roteamento por geoproximidade não pode conter dois ou mais locais que estejam geograficamente situados na mesma área metropolitana. Além disso, algumas Regiões da AWS Zonas Locais, como Oeste dos EUA (Oregon) e Portland, EUA, estão situadas muito próximas umas das outras para serem usadas dentro da mesma política de roteamento por geoproximidade. Se você precisar de roteamento de tráfego para mais de um local na mesma área metropolitana, defina uma política de roteamento por geoproximidade que resulte em uma regra de roteamento ponderado (WRR) 50/50 para dois endpoints diferentes na área, distribuindo assim o tráfego uniformemente entre esses endpoints.

Coordenadas

Se você escolher Custom (enter coordinates) para Endpoint location, insira a latitude e a longitude do local do recurso. Observe o seguinte:

- A latitude representa a localização sul (negativa) ou norte (positiva) da linha do Equador. Os valores válidos são de -90 graus a 90 graus.
- A longitude representa a localização oeste (negativa) ou leste (positiva) do primeiro meridiano. Os valores válidos são de -180 graus a 180 graus.
- Você pode obter a latitude e a longitude em alguns aplicativos de mapas online. Por exemplo, no Google Maps, a URL de um local especifica a latitude e a longitude:

  https://www.google.com/maps/@47.6086111,-122.3409953,20z
- Você pode inserir até dois decimais de precisão, por exemplo, 47,63. Se você especificar um valor mais preciso, o Route 53 truncará o valor para duas casas decimais. Para a latitude e a longitude na linha do Equador, 0,01 graus é de aproximadamente 0,69 quilômetro.

Viés

Opcionalmente, para alterar o tamanho da região geográfica da qual o Route 53 encaminha o tráfego para um recurso, especifique o valor aplicável para o Bias (Desvio):

- Para aumentar o tamanho da região geográfica da qual o Route 53 encaminha o tráfego para um recurso, especifique um inteiro positivo de 1 a 99 para o desvio. O Route 53 diminui o tamanho das regiões adjacentes.
- Para reduzir o tamanho da região geográfica da qual o Route 53 encaminham o tráfego para um recurso, especifique um inteiro negativo de -1 a -99 para o desvio. O Route 53 aumenta o tamanho das regiões adjacentes.

> **Important**
>
> O efeito de alterar o valor do Bias (Desvio) é relativo, com base na localização de outros recursos, em vez de absoluto, com base na distância. Como resultado, é difícil prever o efeito de uma alteração. Por exemplo, dependendo de onde seus recursos estão, alterar o desvio de 10 para 15 pode significar a diferença entre a adição ou a subtração de uma quantidade significativa de tráfego da área metropolitana da cidade de Nova York. Recomendamos que você altere o desvio em pequenos incrementos e avalie os resultados e, em seguida, faça alterações adicionais, se for necessário.

Para ter mais informações, consulte Roteamento por geoproximidade.

Regra de resposta com valores múltiplos

Escolha essa opção quando quiser que o Route 53 responda às consultas ao DNS com até oito respostas íntegras selecionadas de maneira mais ou menos aleatória.

Para ter mais informações, consulte Roteamento de resposta com vários valores.

Regra ponderada

Escolha essa opção quando tiver vários recursos que executam a mesma função (por exemplo, servidores Web que atendem o mesmo site) e quiser que o Route 53 encaminhe tráfego para esses recursos nas proporções que você especificar (por exemplo, 1/3 para um servidor e 2/3 para o outro).

Ao selecionar Weighted rule (Regra ponderada), insira a ponderação que você deseja aplicar a essa regra.

Para ter mais informações, consulte Roteamento ponderado.

Endpoint

Escolha essa opção para especificar o recurso, como uma CloudFront distribuição ou um balanceador de carga do Elastic Load Balancing, para o qual você deseja encaminhar as consultas de DNS.

Regra existente

Escolha essa opção quando você quiser rotear as consultas de DNS para uma regra existente nesta política de tráfego. Por exemplo, você pode criar duas ou mais regras de localização geográfica que roteiam as consultas para países diferentes para a mesma regra de failover. A regra de failover então pode rotear as consultas para dois balanceadores de carga de Elastic Load Balancing.

Esta opção não está disponível se a política de tráfego não incluir quaisquer regras.

Endpoint existente

Escolha essa opção quando quiser rotear consultas de DNS para um endpoint existente. Por exemplo, se você tiver duas regras de failover, talvez queira rotear consultas ao DNS para ambas as opções Em failover (secundário) para o mesmo balanceador de carga de Elastic Load Balancing.

Esta opção não está disponível se a política de tráfego não incluir endpoints.

Tipo de valor

Escolha a opção aplicável:

CloudFront distribuição

Escolha essa opção se quiser rotear o tráfego para uma CloudFront distribuição. A opção só está disponível se você escolheu A: endereço IP no formato IPv4 para Tipo de DNS ou AAAA: endereço IP no formato IPv6 para Tipo de DNS.

Application Load Balancer de ELB

Escolha essa opção se você quiser rotear o tráfego para um Application Load Balancer de Elastic Load Balancing. A opção está disponível somente se você escolheu o A: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6 para Tipo de DNS.

Classic Load Balancer de ELB;

Escolha essa opção se você quiser rotear o tráfego para um Classic Load Balancer de Elastic Load Balancing. A opção está disponível somente se você escolheu o A: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6 para Tipo de DNS.

Network Load Balancer de ELB

Escolha essa opção se você quiser rotear o tráfego para um Network Load Balancer de Elastic Load Balancing. A opção está disponível somente se você escolheu o A: endereço IP no formato IPv4 ou AAAA: endereço IP no formato IPv6 para Tipo de DNS.

Ambiente do Elastic Beanstalk

Escolha essa opção se quiser rotear o tráfego para um ambiente do Elastic Beanstalk. Esta opção está disponível somente se você escolher A: endereço IP no formato IPv4 para Tipo de DNS.

Endpoint do site do S3

Escolha esta opção se você quiser encaminhar o tráfego para um bucket do Amazon S3 configurado como um endpoint do site. Esta opção está disponível somente se você escolher A: endereço IP no formato IPv4 para Tipo de DNS.

Digite o valor de Tipo de DNS

Escolha essa opção se quiser que o Route 53 responda às consultas de DNS usando o valor no campo Value (Valor). Por exemplo, se você escolheu A como o valor de Tipo de DNS quando criou esta política de tráfego, esta opção na lista Tipo de valor será Valor tipo A. Isso requer que

você insira um endereço IP no formato IPv4 no campo Value (Valor). O Route 53 responderá às consultas de DNS encaminhadas para esse endpoint com o endereço IP no campo Value (Valor).

Valor

Selecione ou insira um valor com base na opção que você escolheu para o Value type (Tipo de valor):

CloudFront distribuição

Escolha uma CloudFront distribuição na lista de distribuições associadas à AWS conta atual.

Application Load Balancer de ELB

Escolha um balanceador de carga do Elastic Load Balancing Application na lista de balanceadores de carga associados à conta atual. AWS

Classic Load Balancer de ELB;

Escolha um load balancer do Elastic Load Balancing Classic na lista de balanceadores de carga associados à conta atual. AWS

Network Load Balancer de ELB

Escolha um balanceador de carga do Elastic Load Balancing Network na lista de balanceadores de carga associados à conta atual. AWS

Ambiente do Elastic Beanstalk

Escolha um ambiente do Elastic Beanstalk na lista de ambientes associados à Conta da AWS atual.

Endpoint do site do S3

Escolha um bucket do Amazon S3 na lista de buckets do Amazon S3 que estão configurados como endpoints do site e que estão associados à conta atual. AWS

> **Important**
>
> Quando você cria um registro de política com base na política de tráfego, o bucket que você escolher aqui deve corresponder ao nome de domínio (por exemplo, www.exemplo.com) que você especificar para Policy record DNS name no registro de política. Se Value (Valor) e Policy record DNS name (Nome de DNS no registro de

política) não corresponderem, o Amazon S3 não responderá às consultas de DNS do nome de domínio.

Digite o valor de Tipo de DNS

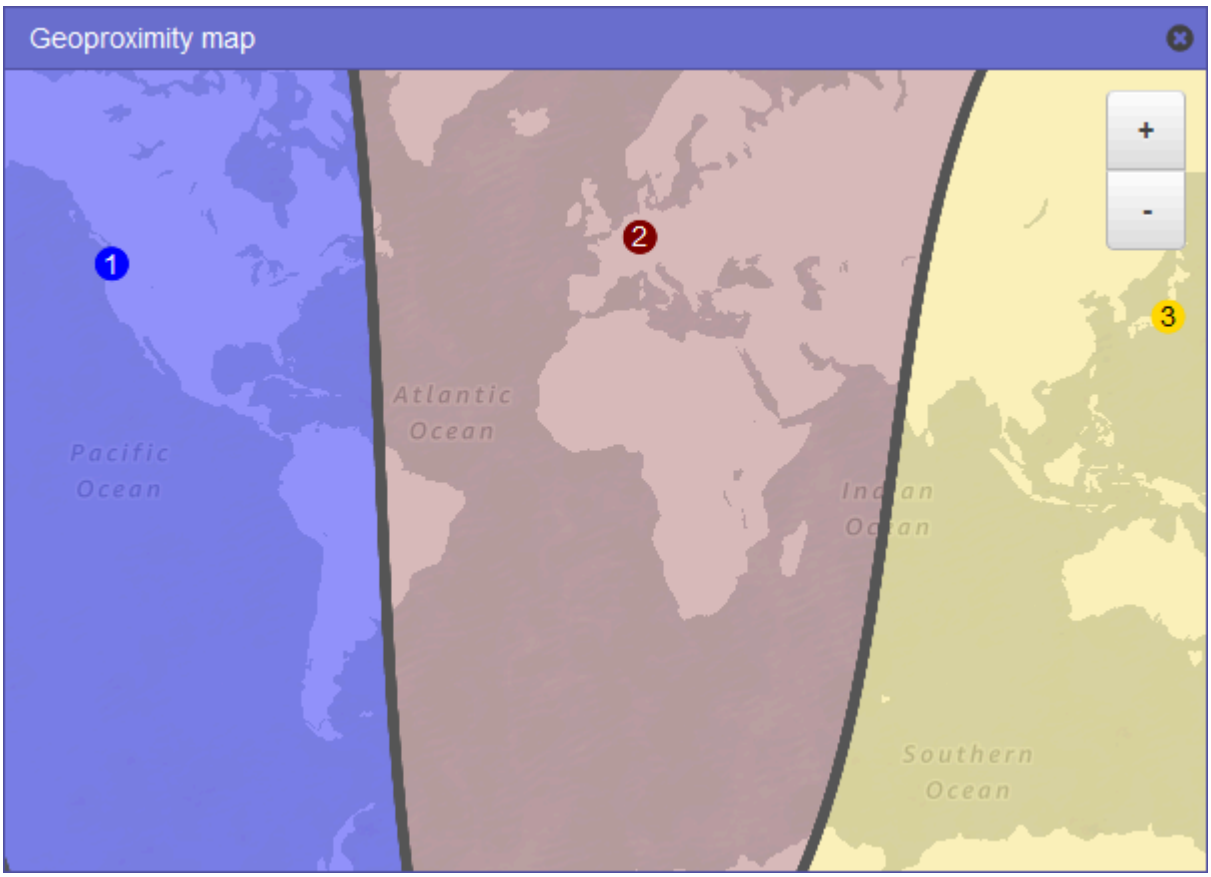
Digite um valor que corresponde ao valor especificado para o Tipo de DNS quando iniciou esta política de tráfego. Por exemplo, se você selecionou MX para o DNS type (Tipo de DNS), insira dois valores: a prioridade que deseja atribuir a um servidor de e-mail e o nome de domínio do servidor de e-mail, como `10 sydney.mail.example.com`.

Para obter mais informações sobre os tipos de DNS com suporte, consulte Tipos de registro de DNS com suporte.

Visualizar um mapa que mostra o efeito das configurações de geoproximidade

Uma regra de geoproximidade permite que você especifique as localizações de seus recursos, tanto em Regiões da AWS Zonas Locais quanto em Zonas Locais e, usando latitude e longitude, em locais não localizados.AWS Quando você cria uma regra de geoproximity, o Route 53 encaminha o tráfego de Internet para o recurso mais próximo de seus usuários. Você também pode optar por rotear mais ou menos tráfego para um recurso especificando um desvio que aumenta ou diminui o tamanho da área geográfica da qual o tráfego é roteado para um recurso. Para obter mais informações sobre roteamento de geoproximity, consulte Roteamento por geoproximidade.

Você pode exibir um mapa que mostra o efeito de suas configurações de geoproximity atuais. Por exemplo, se você tiver recursos nas regiões Oeste dos EUA (Oregon), Europa (Frankfurt) e Ásia-Pacífico (Tóquio) e não especificar um desvio, essa será a aparência do mapa.



Para exibir o mapa de para uma regra de geoproximity, selecione o ícone de gráfico ao lado de Mostrar mapa de geoproximity. (Esse ícone aparece na parte superior da regra.) Para ocultar o mapa, selecione o ícone novamente ou selecione o x no canto superior direito do mapa.

Observe o seguinte:

- O mapa é preciso dentro de aproximadamente 10 milhas (16 quilômetros).
- O mapa ajusta automaticamente quando você adicionar, editar ou excluir regiões, ou quando você alterar a configuração de desvio de uma região.
- A número e cor da região em cada definição de regra correspondem aos números e cores no mapa.
- Você pode aumentar e diminuir o zoom para ver mais ou menos detalhes. Use os botões + e - no mapa, um touchpad ou roda em um mouse para alterar o nível de zoom.
- Você pode mover o mapa dentro da janela do mapa para ver áreas específicas. Use um touchpad ou clique e arraste o mapa com o mouse. Também é possível mover a janela do mapa em uma janela do navegador.

- Se tiver mais de uma regra de geoproximity em uma política, você poderá visualizar o mapa para somente uma regra por vez.

Criar versões adicionais de uma política de tráfego

Quando você edita uma política de tráfego, o Amazon Route 53 cria automaticamente outra versão da política de tráfego e mantém as versões anteriores, a menos que você opte por excluí-las. A nova versão tem o mesmo nome da política de tráfego que você está editando e se diferencia da versão original por um número de versão que o Route 53 incrementa automaticamente. Você pode basear a nova versão de uma política de tráfego em qualquer versão existente de uma política de tráfego que tenha o mesmo nome.

O Route 53 não reutiliza os números de versão para novas versões de uma determinada política de tráfego. Por exemplo, se você criar três versões da MyTrafficPolítica, excluir as duas últimas versões e depois criar outra versão, a nova versão será a versão 4. Ao manter as versões anteriores, o Route 53 garante que você pode reverter para uma configuração anterior se uma nova configuração não encaminhar o tráfego, conforme desejado.

Para criar uma nova versão de política de tráfego, execute o procedimento a seguir.

Para criar outra versão de uma política de tráfego

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Políticas de tráfego.
3. Selecione o nome da política de tráfego da qual deseja criar uma nova versão.
4. Na tabela Versões da política de tráfego na parte superior da página, marque a caixa de seleção da versão da política de tráfego que deseja usar como base para a nova versão de política de tráfego.
5. Escolha Editar política como nova versão.
6. Na página Update description (Atualizar descrição), insira uma descrição para a nova versão da política de tráfego. Recomendamos que você especifique uma descrição que diferencie esta versão de outras versões da mesma política de tráfego. Quando você cria um novo registro de política, o valor especificado aparece na lista de versões disponíveis para esta política de tráfego.
7. Selecione Next (Próximo).

8. Atualize a configuração conforme aplicável. Para ter mais informações, consulte Valores que você especifica quando cria uma política de tráfego.

   Você pode excluir regras, endpoints e ramificações de uma política de tráfego das seguintes formas:

   - Para excluir uma regra ou endpoint, clique no x no canto superior direito da caixa.

     > **Important**
     >
     > Se você excluir uma regra que tem regras filho e endpoints, o Route 53 também excluirá todos os filhos.

   - Se você conectar duas regras à mesma regra filho ou endpoint e quiser excluir uma das conexões, posicione o cursor na conexão que deseja excluir e clique no x da conexão.
9. Quando terminar a edição, escolha Salvar como nova versão.
10. Opcional: especifique as configurações para criar um ou mais registros de política em uma zona hospedada usando a nova versão de política de tráfego. Para ter mais informações, consulte Valores que você especifica quando cria ou atualiza um registro de política. Você também pode criar registros de política mais tarde, na mesma zona hospedada ou em zonas hospedadas adicionais.

    Se você não quiser criar registros de política agora, escolha Ignorar esta etapa e o console exibirá a lista de políticas de tráfego e registros de políticas que você criou usando a AWS conta atual.
11. Se você especificou configurações para os registros de política na etapa anterior, escolha Criar registro de política.

Criar uma política de tráfego por meio da importação de um documento JSON

Você pode criar uma nova política de tráfego ou uma nova versão de uma política de tráfego existente importando um documento em formato JSON que descreve todos os endpoints e as regras que você deseja incluir na política de tráfego. Para obter informações sobre o formato de documento JSON e vários exemplos que você pode copiar e rever, consulte Formato do documento da política de tráfego na Referência da API do Amazon Route 53.

A maneira mais fácil de obter o documento formatado em JSON para uma versão existente da política de tráfego é usar o comando `get-traffic-policy` na CLI. AWS Para obter mais informações, consulte get-traffic-policy na Referência de comando da AWS CLI .

O arquivo JSON criado pelo comando `get-traffic-policy` inclui barras invertidas (\) como caracteres de escape. Antes de importar o arquivo JSON, substitua todas as barras invertidas por caracteres nulos.

Para criar uma política de tráfego por meio da importação de um documento JSON

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Para criar uma nova política de tráfego importando um documento JSON, execute as seguintes etapas:
   a. No painel de navegação, selecione Políticas de tráfego.
   b. Selecione Criar política de tráfego.
   c. Na página Política de nome, especifique os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica quando cria uma política de tráfego.
   d. Vá para a etapa 4.
3. Para criar uma nova versão de uma política de tráfego existente importando um documento JSON, execute as seguintes etapas:
   a. No painel de navegação, selecione Políticas de tráfego.
   b. Selecione o nome da política de tráfego na qual deseja basear a nova versão.
   c. Na tabela Versões da política de tráfego, marque a caixa de seleção da versão na qual deseja basear a nova versão.
   d. Escolha Editar política como nova versão.
   e. Na página Update description (Atualizar descrição), insira uma descrição para a nova versão.
   f. Vá para a etapa 4.
4. Selecione Next (Próximo).
5. Selecione Importar política de tráfego.
6. Insira uma nova política de tráfego, cole uma política de tráfego de exemplo ou uma política de tráfego existente.

7. Selecione Importar política de tráfego.

Visualizar versões de política de tráfego e registros de política associados

Você pode ver todas as versões criadas para uma política de tráfego, bem como todos os registros de política criados usando cada uma das versões da política de tráfego.

Para visualizar versões de política de tráfego e registros de política associados

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Políticas de tráfego.
3. Escolha o nome de uma política de tráfego.
4. A tabela superior lista todas as versões que você criou de uma política de tráfego. A tabela inclui as seguintes informações:

   Número da versão

   O número de cada versão de uma política de tráfego que você criou. Se você escolher o número da versão, o console exibirá a configuração para essa versão.

   Número de registros de política

   O número de registros de política que você criou usando esta versão de política de tráfego.

   Tipo de DNS

   O tipo de DNS que você especificou quando criou a versão da política de tráfego.

   Descrição da versão

   A descrição que você especificou quando criou a versão da política de tráfego.
5. A tabela inferior lista todos os registros de política que você criou usando as versões de política de tráfego na tabela superior. A tabela inclui as seguintes informações:

   Nome de DNS do registro de política

   Os nomes de DNS aos quais você associou a política de tráfego.

   Status

   Os valores possíveis incluem o seguinte:

Aplicado

O Route 53 concluiu a criação ou atualização de um registro de política e dos registros correspondentes.

Criando

O Route 53 está criando os registros para um novo registro de política.

Atualizando

Você atualizou um registro de política e o Route 53 está criando de um novo grupo de registros que substituirá o grupo existente de registros para o nome de DNS.

Excluindo

O Route 53 está excluindo um registro de política e os registros associados.

Com falha

O Route 53 não foi capaz de criar ou atualizar o registro de política e os registros associados.

Versão usada

Indica a versão da política de tráfego que você usou para criar o registro de política.

Tipo de DNS

O tipo de DNS de todos os registros que o Route 53 criou para esse registro de política. Quando você edita um registro de política, deve especificar uma versão de política de tráfego que tem o mesmo tipo de DNS como o tipo de DNS para o registro de política que está editando.

TTL (em segundos)

A quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172.800 segundos ou dois dias), pagará menos pelo serviço do Route 53, pois os resolvers recursivos enviarão solicitações ao Route 53 com menos frequência. No entanto, as alterações nos registros (por exemplo, um novo endereço IP) levarão mais tempo para serem aplicadas, pois os resolvedores recursivos usarão os valores em cache por períodos mais longos, em vez de solicitar as informações mais recentes ao Route 53.

Excluir versões da política de tráfego e políticas de tráfego

Para excluir uma política de tráfego, você deve excluir todas as versões (incluindo o original) criadas para a política de tráfego. Além disso, para excluir uma versão de política de tráfego, você deve excluir todos os registros de política criados com a versão da política de tráfego.

> **Important**
>
> Se você excluir registros de política que o Amazon Route 53 está usando para responder a consultas de DNS, o Route 53 parará de responder a consultas para os nomes DNS correspondentes. Por exemplo, se o Route 53 estiver usando o registro de política para www.exemplo.com para responder às consultas de DNS para www.exemplo.com e você excluir o registro de política, os usuários não poderão acessar seu site ou aplicação Web usando o nome de domínio www.exemplo.com.

Para excluir versões de política de tráfego e, opcionalmente, uma política de tráfego, execute o procedimento a seguir:

Para excluir versões da política de tráfego e uma política de tráfego

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Políticas de tráfego.
3. Escolha o nome da política de tráfego para a qual você deseja excluir as versões de política de tráfego e que, opcionalmente, você deseja excluir por completo.
4. Se as versões da política de tráfego que você deseja excluir na tabela superior forem exibidas na coluna Versão usada da tabela inferior, marque as caixas de seleção dos registros de política correspondentes na tabela inferior.

   Por exemplo, se você deseja excluir a versão 3 de uma política de tráfego, mas criou um dos registros de política na tabela inferior usando versão 3, marque a caixa de seleção deste registro de política.
5. Escolha Excluir registros de política.
6. Escolha o botão atualizar para que a tabela inferior atualize a exibição até que os registros de política excluídos não apareçam mais na tabela.

7. Na tabela superior, marque as caixa de seleção das versões de política de tráfego que deseja excluir.
8. Selecione Excluir versão.
9. Se você tiver excluído todas as versões de política de tráfego na etapa anterior e também quiser excluir a política de tráfego, selecione o botão atualizar da tabela superior para atualizar a exibição até que a tabela fique vazia.
10. No painel de navegação, selecione Políticas de tráfego.
11. Na lista de políticas de tráfego, marque a caixa de seleção da política de tráfego que você deseja excluir.
12. Selecione Excluir política de tráfego.

Criar e gerenciar registros de política

Para rotear o tráfego de Internet para os recursos especificados ao criar uma política de tráfego, você cria um ou mais registros de política. Cada registro de política identifica a zona hospedada na qual você deseja criar o registro de política e o nome de domínio ou subdomínio para o qual você deseja rotear o tráfego. Por exemplo, se você deseja rotear o tráfego para www.example.com, especifique o ID da zona hospedada para a zona hospedada example.com, e especifique www.example.com em Policy record DNS name (Nome de DNS no registro de política).

Se você quiser usar a mesma política de tráfego para rotear o tráfego para mais de um nome de domínio ou subdomínio, você tem duas opções:

- Você pode criar um registro de política para cada nome de domínio ou subdomínio.
- Você pode criar um registro de política e criar registros CNAME ou de alias que se referem ao registro de política.

Por exemplo, se você quiser usar a mesma política de tráfego para example.com, example.org e example.net, poderá executar uma das seguintes ações:

- Criar um registro de política para cada um deles.
- Criar um registro de política para um deles e criar registros CNAME em zonas hospedadas para as outras duas. Nos dois registros CNAME, você especifica o nome do registro para o qual criou um registro de política.

Se você quiser usar a mesma política de tráfego para um domínio e os subdomínios dele, como example.com e www.example.com, poderá criar um registro de política para um nome e registros de alias para o restante. Por exemplo, você pode criar um registro de política para example.com e criar um registro de alias de www.example.com que tenha o registro example.com como destino do alias.

> **Note**
>
> Para cada registro de política criado, será cobrada uma taxa mensal. Se você quiser usar a mesma política de tráfego para vários nomes de domínio ou subdomínio, pode usar CNAME ou registros de alias para reduzir suas cobranças:
>
> - Se você criar um registro de política e um ou mais registros CNAME que se referem ao registro de política, pagará apenas pelo registro de política e pelas consultas de DNS para os registros CNAME.
> - Se você criar um registro de política e um ou mais registros de alias na mesma zona hospedada que se referem ao registro de política, você pagará apenas pelo registro de política e pelas consultas de DNS para o registro de alias.

Tópicos

Criar registros de política

Para criar um registro de política, execute o procedimento a seguir.

> **Important**
>
> Para cada registro de política criado, será cobrada uma taxa mensal. Se, posteriormente, você excluir o registro de política, a cobrança será feita proporcionalmente. Para obter mais informações, consulte a seção “Fluxo de tráfego” da página Preços do Amazon Route 53.

Para criar um registro de política

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Registros de política.
3. Na página Registros de política, escolha Criar registros de política.
4. Na página Criar registros de política, especifique os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica quando cria ou atualiza um registro de política.
5. Escolha Criar registros de política.

   Pode levar vários minutos para o status do registro de política criado ser exibido como Aplicado.
6. Se quiser criar registros de política em outra zona hospedada, repita as etapas de 3 a 5.

> **Note**
>
> Se o status do registro da política for Falha, escolha o botão de informações ao lado do status para obter mais informações sobre a falha. Se precisar de mais ajuda e quiser entrar em contato com o AWS suporte, consulte Como faço para obter suporte técnico AWS?

Valores que você especifica quando cria ou atualiza um registro de política

Quando você cria ou atualiza um registro de política, especifica os valores a seguir

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

Política de tráfego

Escolha a política de tráfego cuja configuração deseja usar para este registro de política.

Versão

Escolha a versão da política de tráfego cuja configuração deseja usar para este registro de política.

Se você estiver atualizando um registro de política existente, deve escolher uma versão para a qual o tipo de DNS corresponde ao tipo de DNS atual do registro de política. Por exemplo, se o tipo de DNS do registro de política é A, escolha uma versão para a qual o tipo de DNS é A.

Zona hospedada

Escolha a zona hospedada em que você deseja criar um registro de política usando a política de tráfego especificada e versão. Você não pode alterar o valor da zona hospedada depois que criar um registro de política.

Nome de DNS do registro de política

Quando você estiver criando um registro de política, insira o nome de domínio ou subdomínio para o qual deseja que o Route 53 responda às consultas de DNS usando a configuração na política e versão de tráfego especificadas.

Para usar a mesma configuração para mais de um nome de domínio ou subdomínio na zona hospedada especificada, escolha Adicionar outro registro de política e digite o nome de domínio ou subdomínio aplicável assim como o TTL.

Você não pode alterar o valor de Nome de DNS no registro de política depois que criar um registro de política.

TTL (em segundos)

Insira a quantidade de tempo, em segundos, que você deseja que os resolvedores recursivos de DNS armazenem informações em cache sobre esse registro. Se você especificar um valor mais longo (por exemplo, 172.800 segundos ou dois dias), você pagará menos pelo serviço do Route 53, pois os resolvedores recursivos enviarão solicitações ao Route 53 com menos frequência. No entanto, as alterações nos registros (por exemplo, um novo endereço IP) levarão mais tempo para serem aplicadas, pois os resolvedores recursivos usarão os valores em cache por períodos mais longos, em vez de solicitar as informações mais recentes ao Route 53.

Atualizar registros de política

Para atualizar as configurações em um registro de política, execute o procedimento a seguir.

Para atualizar um registro de política

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Registros de política.
3. Na página Registros de política, marque a caixa de seleção do registro de política que você deseja atualizar e selecione Editar registro de política.
4. Na página Editar registro de política, especifique os valores aplicáveis. Para ter mais informações, consulte Valores que você especifica quando cria ou atualiza um registro de política.
5. Escolha Editar registro de política.

   Pode levar vários minutos para o status do registro de política criado ser exibido como Aplicado.
6. Se quiser atualizar outro registro de política, repita as etapas de 3 a 5.

> **Note**
>
> Se o status do registro da política for Falha, escolha o botão de informações ao lado do status para obter mais informações sobre a falha. Se precisar de mais ajuda e quiser entrar em contato com o AWS suporte, consulte Como faço para obter suporte técnico AWS?

Excluir registros de política

Para excluir registros de política, execute o procedimento a seguir.

> **Important**
>
> Se você excluir registros de política que o Amazon Route 53 está usando para responder a consultas de DNS, o Route 53 parará de responder a consultas para os nomes DNS correspondentes. Por exemplo, se o Route 53 estiver usando o registro de política para www.exemplo.com para responder às consultas de DNS para www.exemplo.com e você excluir o registro de política, os usuários não poderão acessar seu site ou aplicação Web usando o nome de domínio www.exemplo.com.

Para excluir um registro de política

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Registros de política.
3. Na página Registros de política, marque as caixas de seleção dos registros de política que você deseja excluir e selecione Excluir registro de política.

   Aguarde alguns minutos e atualize a página para garantir que o registro da política desapareça da lista.

O que Amazon Route 53 Resolveré

Amazon Route 53 Resolver responde recursivamente às consultas de DNS de AWS recursos para registros públicos, nomes DNS específicos do Amazon VPC e zonas hospedadas privadas do Amazon Route 53, e está disponível por padrão em todas as VPCs.

> **Note**
>
> Amazon Route 53 Resolver anteriormente era chamado de servidor Amazon DNS, mas foi renomeado quando as regras do Resolver e os endpoints de entrada e saída foram introduzidos. Para obter mais informações, consulte servidor Amazon DNS no Guia do usuário da Amazon Virtual Private Cloud.

Uma Amazon VPC se conecta a um Route 53 Resolver em um endereço IP VPC+2. Esse endereço VPC+2 se conecta a um Route 53 Resolver dentro de uma zona de disponibilidade.

O Route 53 Resolver responde automaticamente às consultas ao DNS para:

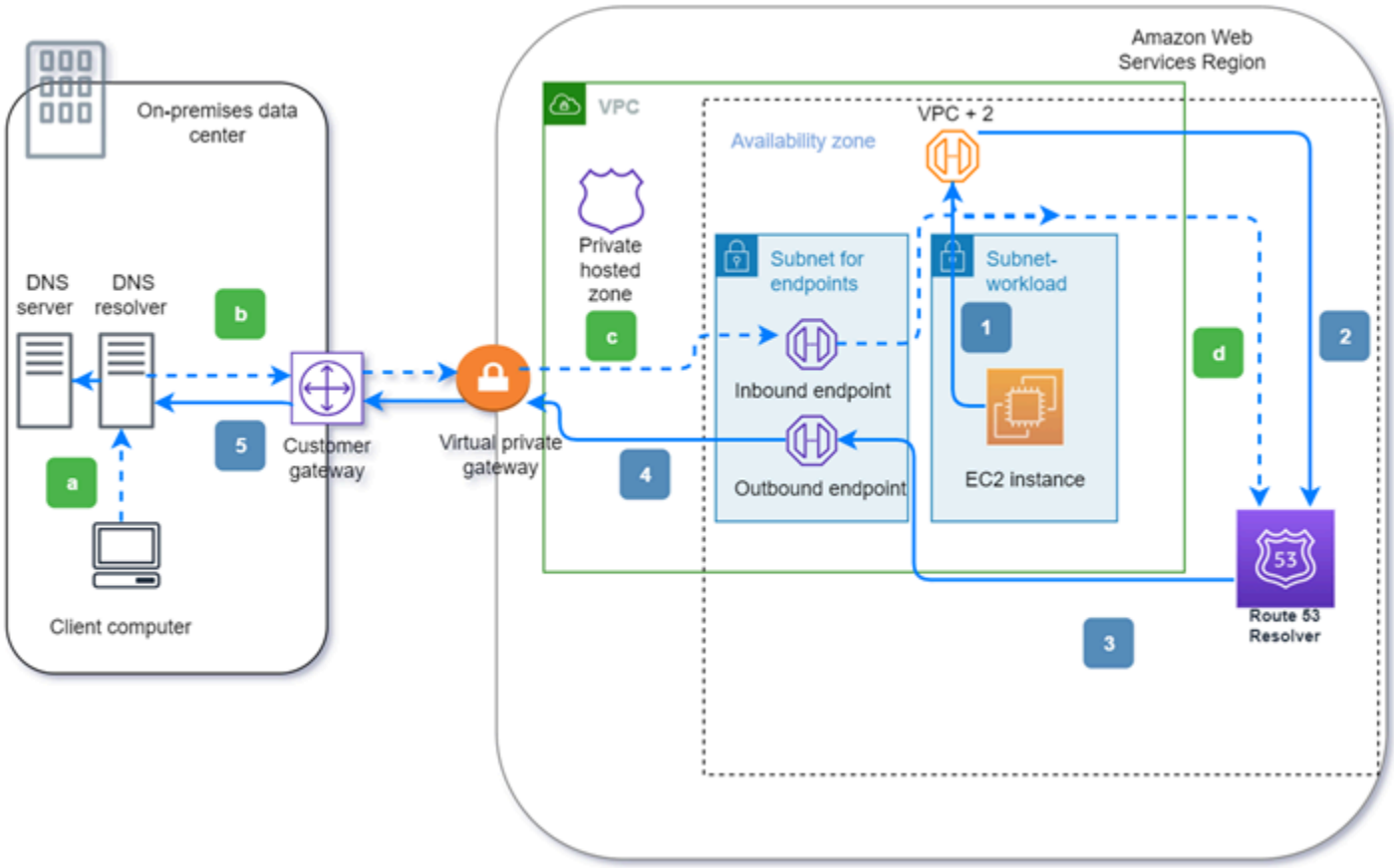
- Nomes de domínio de VPC locais para instâncias do EC2 (por exemplo, ec2-192-0-2-44.compute-1.amazonaws.com).
- Registros em zonas hospedadas privadas (por exemplo, acme.exemplo.com).
- Para todos os outros nomes de domínios, o Route 53 Resolver faz pesquisas recursivas em servidores de nomes públicos.

Se tiver cargas de trabalho que utilizem tanto VPCs quanto recursos locais, você também precisará resolver os registros DNS hospedados on-premises. Da mesma forma, esses recursos locais podem precisar resolver nomes hospedados em AWS. Por meio de endpoints do Resolver e de regras de encaminhamento condicional, você pode resolver consultas ao DNS entre os recursos on-premises e as VPCs para criar uma configuração de nuvem híbrida por VPN ou Direct Connect (DX). Especificamente:

- Os endpoints de entrada do Resolver permitem consultas ao DNS à VPC, originadas na rede on-premises ou em outra VPC.

- Os endpoints de saída do Resolver permitem consultas ao DNS da VPC para a rede on-premises ou para outra VPC.
- As regras do Resolver permitem que você crie uma regra de encaminhamento para cada nome de domínio e especifique o nome do domínio para o qual deseja encaminhar as consultas ao DNS da VPC para um resolvedor de DNS on-premises e do resolvedor on-premises para a VPC. As regras são aplicadas diretamente à VPC e podem ser compartilhadas entre várias contas.

O diagrama a seguir mostra a resolução de DNS híbrido com endpoints do Resolver. Observe que o diagrama é simplificado para mostrar somente uma zona de disponibilidade.



O diagrama ilustra as seguintes etapas:

Saída (setas cheias 1 a 5):

1. Uma instância do Amazon EC2 precisa resolver uma consulta ao DNS para o domínio interno.exemplo.com. O servidor DNS confiável está no datacenter on-premises. Essa consulta ao DNS é enviada para VPC+2 na VPC que se conecta ao Route 53 Resolver.

2. Uma regra de encaminhamento do Route 53 Resolver está configurada para encaminhar consultas para interno.exemplo.com no datacenter on-premises.
3. A consulta é encaminhada para um endpoint externo.
4. O endpoint de saída encaminha a consulta para o resolvedor de DNS local por meio de uma conexão privada entre AWS e o data center. A conexão pode ser AWS Direct Connect ou AWS Site-to-Site VPN descrita como um gateway privado virtual.
5. O resolvedor de DNS on-premises resolve a consulta ao DNS para interno.exemplo.com e retorna a resposta para a instância do Amazon EC2 pelo caminho inverso.

Entrada (setas tracejadas a — d):

a. Um cliente no data center local precisa resolver uma consulta de DNS para um AWS recurso do domínio dev.example.com. Ele envia a consulta para o resolvedor de DNS on-premises.
b. O resolvedor de DNS on-premises tem uma regra de encaminhamento que direciona as consultas a dev.exemplo.com para um endpoint de entrada.
c. A consulta chega ao endpoint de entrada por meio de uma conexão privada, como AWS Direct Connect ou AWS Site-to-Site VPN, descrita como um gateway virtual.
d. O endpoint de entrada envia a consulta para o Route 53 Resolver, e o Route 53 Resolver resolve a consulta DNS para dev.example.com e retorna a resposta ao cliente pelo mesmo caminho inverso.

Tópicos

Resolver consultas de DNS entre VPCs e sua rede

Além disso, o Resolver contém endpoints configurados para responder a consultas ao DNS para e do ambiente on-premises.

> **Note**
>
> O encaminhamento de consultas ao DNS privadas para qualquer endereço VPC CIDR + 2 de seus servidores DNS on-premises não é suportado e pode causar resultados instáveis. Em vez disso, recomendamos o uso de um endpoint de entrada do Resolver.

Também é possível integrar a resolução de DNS entre os resolvedores de DNS e o Resolver na sua rede, configurando regras de encaminhamento. Sua rede pode incluir qualquer rede acessível de sua VPC, como o seguinte:

- A própria VPC
- Outra VPC emparelhada
- Uma rede local conectada a uma VPN ou AWS a AWS Direct Connect um gateway de conversão de endereços de rede (NAT)

Antes de começar a encaminhar consultas, crie endpoints de entrada e/ou saída do Resolver na VPC conectada. Esses endpoints fornecem um caminho para consultas de entrada ou saída:

Endpoint de entrada: os resolvedores de DNS em sua rede podem encaminhar consultas de DNS para o Route 53 Resolver, por meio desse endpoint

Isso permite que seus resolvedores de DNS resolvam facilmente nomes de domínio para AWS recursos como instâncias do EC2 ou registros em uma zona hospedada privada do Route 53. Para ter mais informações, consulte Como resolvedores de DNS em sua rede encaminham consultas de DNS para endpoints do Route 53 Resolver.

Endpoint de saída: o Resolver encaminha condicionalmente consultas para resolvedores em sua rede por meio desse endpoint

Para encaminhar consultas selecionadas, crie regras do Resolver que especificam os nomes de domínio para as consultas de DNS que você quer encaminhar (como example.com) e os endereços IP dos resolvedores de DNS na rede para os quais você quer encaminhar as

consultas. Se uma consulta corresponder a várias regras (example.com, acme.example.com), o Resolver escolherá a regra com a correspondência mais específica (acme.example.com) e encaminhará a consulta aos endereços IP especificados nessa regra. Para ter mais informações, consulte Como o endpoint do Route 53 Resolver encaminha consultas de DNS das VPCs para a rede.

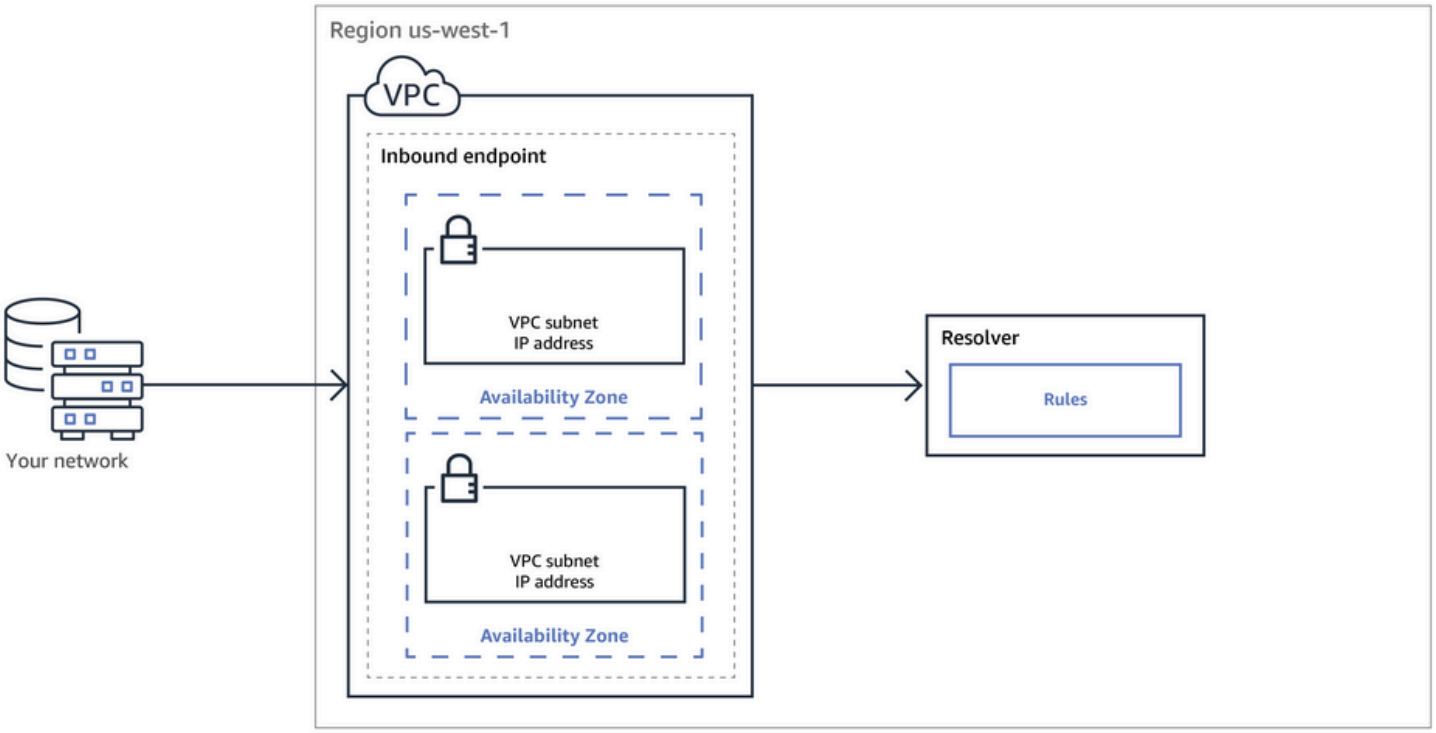
Assim como a Amazon VPC, o Resolver é regional. Em cada região em que possua VPCs, você pode escolher se deseja encaminhar consultas de suas VPCs à rede (consultas de saída), da rede para as VPCs (consultas de entrada), ou ambos.

Você não pode criar endpoints do Resolver em uma VPC que não seja sua. Somente o proprietário da VPC pode criar recursos de nível de VPC, como endpoints de entrada.

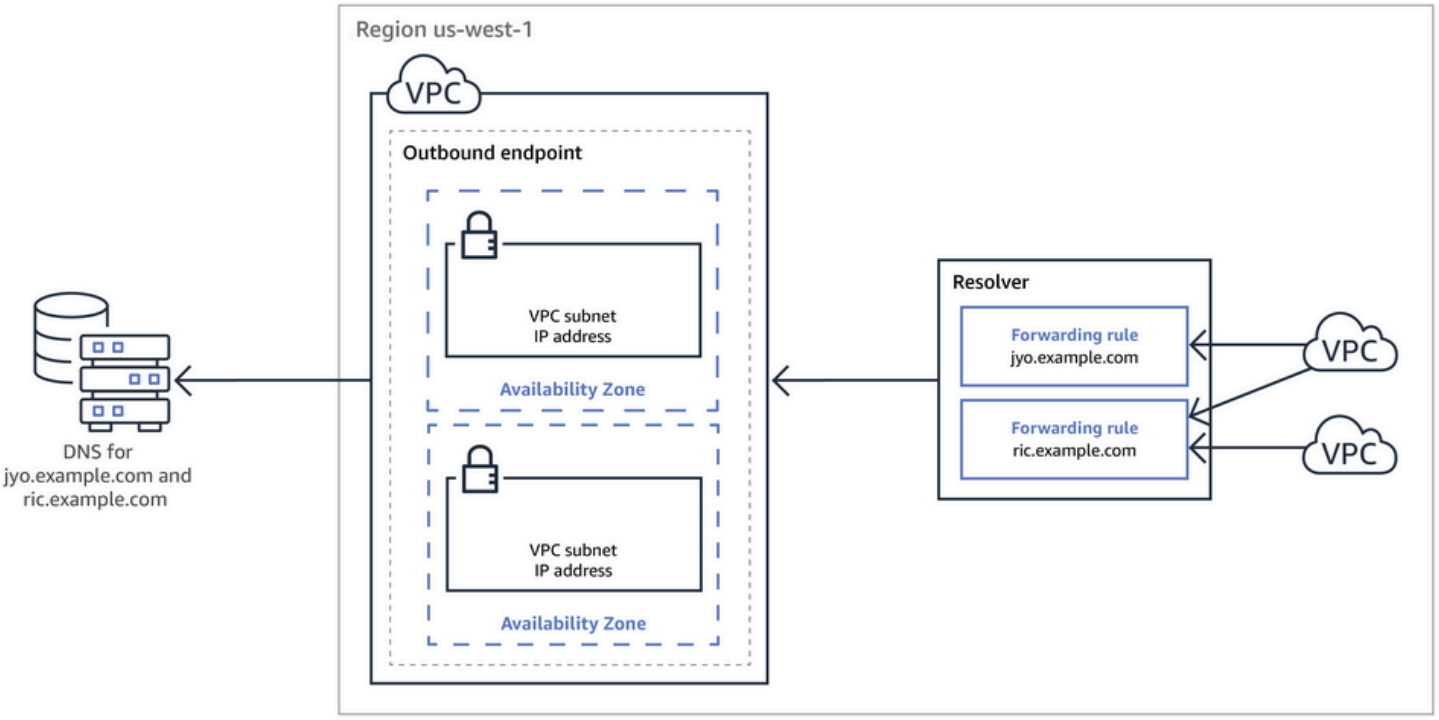
> **Note**
>
> Quando você cria um endpoint do Resolver, não é possível especificar uma VPC que tenha o atributo de locação de instância definido como `dedicated`. Para ter mais informações, consulte .

Para usar o encaminhamento de entrada ou de saída, crie um endpoint do Resolver na VPC. Como parte da definição de um endpoint, especifique os endereços IP para os quais deseja encaminhar consultas de DNS de entrada ou os endereços IP dos quais deseja que as consultas de saída sejam originadas. Para cada endereço IP especificado, o Resolver cria automaticamente uma interface de rede elástica da VPC.

O diagrama a seguir mostra o caminho de uma consulta de DNS de um resolvedor de DNS na rede para endpoints do Route 53 Resolver.



O diagrama a seguir mostra o caminho de uma consulta de DNS a partir de uma instância do EC2 em uma das VPCs para um resolvedor de DNS na rede.



Para obter uma visão geral sobre interfaces de rede da VPC, consulte Interfaces de rede elástica no Manual do usuário da Amazon VPC.

Tópicos

Como resolvedores de DNS em sua rede encaminham consultas de DNS para endpoints do Route 53 Resolver

Quando quiser encaminhar consultas de DNS de sua rede para o Route 53 Resolver em uma região da AWS , execute as seguintes etapas:

1. Você cria um endpoint de entrada do Route 53 Resolver em uma VPC e especifica os endereços IP para os quais os resolvedores em sua rede encaminham consultas de DNS.

   Para cada endereço IP que você especificar para o endpoint de entrada, o Resolver criará uma interface de rede elástica da VPC na VPC em que você criou o endpoint de entrada.
2. Configure os resolvedores na rede para encaminhar consultas de DNS dos nomes de domínio aplicáveis para os endereços IP especificados no endpoint de entrada. Para ter mais informações, consulte Considerações ao criar endpoints de entrada e de saída.

Veja como o Resolver resolve consultas de DNS que se originam na rede:

1. Um navegador da Web ou outra aplicação da rede envia uma consulta de DNS para um nome de domínio encaminhado ao Resolver.
2. Um resolvedor na rede encaminha a consulta para os endereços IP no endpoint de entrada.
3. O endpoint de entrada encaminha a consulta ao Resolver.
4. O Resolver obtém o valor aplicável para o nome de domínio na consulta de DNS, internamente ou executando uma busca recursiva nos servidores de nome público.
5. O Resolver retorna o valor para o endpoint de entrada.
6. O endpoint de entrada retorna o valor ao resolvedor na rede.
7. O resolvedor na rede retorna o valor ao aplicativo.
8. Usando o valor que foi retornado pelo Resolver, a aplicação envia uma solicitação HTTP, por exemplo, uma solicitação para um objeto em um bucket do Amazon S3.

A criação de um endpoint de entrada não altera o comportamento do Resolver, apenas fornece um caminho de um local fora da AWS rede até o Resolver.

Como o endpoint do Route 53 Resolver encaminha consultas de DNS das VPCs para a rede

Quando você quiser encaminhar consultas de DNS das instâncias do EC2 em uma ou mais VPCs em uma AWS região para sua rede, execute as etapas a seguir.

1. Você cria um endpoint de saída do Route 53 Resolver em uma VPC e especifica diversos valores:
   - A VPC pela qual deseja que as consultas de DNS passem a caminho dos resolvedores em sua rede.
   - Os endereços IP na VPC na qual você quer que o Resolver encaminhe as consultas de DNS. Para hosts em sua rede, esses são os endereços IP em que as consultas de DNS se originam.
   - Um grupo de segurança da VPC

   Para cada endereço IP que você especificar para o endpoint de entrada, o Resolver criará uma interface de rede elástica da Amazon VPC na VPC que você especificar. Para ter mais informações, consulte Considerações ao criar endpoints de entrada e de saída.
2. Você cria uma ou mais regras, que especificam os nomes de domínio das consultas de DNS que você quer que o Resolver encaminhe aos resolvedores na rede. Especifique também os endereços IP dos resolvedores. Para ter mais informações, consulte Uso de regras para controlar quais consultas são encaminhadas para sua rede.
3. Associe cada regra às VPCs para as quais você deseja encaminhar consultas de DNS para sua rede.

Tópicos

- Uso de regras para controlar quais consultas são encaminhadas para sua rede
- Como o Resolver determina se o nome do domínio em uma consulta corresponde a uma regra
- Como o Resolver determina para onde encaminhar consultas de DNS
- Usar regras em várias regiões
- Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas

Uso de regras para controlar quais consultas são encaminhadas para sua rede

As regras controlam quais consultas de DNS o endpoint do Route 53 Resolver encaminha aos resolvedores de DNS na rede e quais consultas o Resolver responde por si só.

Você pode categorizar as regras de diversas maneiras. Uma delas é por quem as cria:

- Regras autodefinidas: o Resolver cria automaticamente regras autodefinidas e associa as regras às VPCs. A maioria dessas regras se aplica aos nomes de domínio AWS específicos para os quais o Resolver responde às consultas. Para ter mais informações, consulte Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas.
- Regras personalizadas: você cria regras personalizadas e associa as regras às VPCs. Atualmente, você pode criar apenas um tipo de regra personalizada, regras de encaminhamento condicional, também conhecidas como regras de encaminhamento. O encaminhamento de regras faz com que o Resolver encaminhe consultas de DNS de suas VPCs para os endereços IP dos resolvedores de DNS na rede.

  Se você criar uma regra de encaminhamento para o mesmo domínio como uma regra autodefinida, o Resolver encaminhará as consultas desse nome de domínio para os resolvedores de DNS na rede com base nas configurações da regra de encaminhamento.

Outra maneira de categorizar as regras é pelo que elas fazem:

- Regras de encaminhamento condicional: crie regras de encaminhamento condicional (também conhecidas como regras de encaminhamento) quando quiser encaminhar consultas de DNS de nomes de domínio específicos para resolvedores de DNS na rede.
- Regras do sistema: as regras do sistema fazem com que o Resolver substitua de forma seletiva o comportamento definido em uma regra de encaminhamento. Ao criar uma regra de sistema, o Resolver resolve consultas de DNS de subdomínios especificados que, de outra forma, seriam resolvidas por resolvedores de DNS na rede.

  Por padrão, o encaminhamento de regras se aplica a um nome de domínio e todos os seus subdomínios. Se quiser encaminhar consultas de um domínio para um resolvedor na rede, mas não quiser encaminhar as consultas de alguns subdomínios, crie uma regra de sistema para os subdomínios. Por exemplo, se você criar uma regra de encaminhamento para exemplo.com mas não quiser encaminhar consultas para acme.exemplo.com, crie uma regra de sistema e especifique acme.exemplo.com para o nome de domínio.

- Regra recursiva: o Resolver cria automaticamente uma regra recursiva chamada Internet Resolver (Resolvedor de Internet). Essa regra faz com que o Resolver do Route 53 atue como um resolvedor recursivo para todos os nomes de domínio para os quais você não criou regras personalizadas e para os quais o Resolver não criou regras definidas automaticamente. Para obter informações sobre como substituir esse comportamento, consulte "Encaminhamento de todas as consultas para sua rede" mais adiante neste tópico.

Você pode criar regras personalizadas que se aplicam a nomes de domínio específicos (seus ou a maioria dos nomes de AWS domínio), a nomes de AWS domínios públicos ou a todos os nomes de domínio.

Encaminhamento de consultas de nomes de domínio específicos à rede

Para encaminhar consultas de um nome de domínio específico, como exemplo.com, à sua rede, crie uma regra e especifique esse nome de domínio. Especifique também os endereços IP dos resolvedores de DNS na rede para os quais deseja encaminhar as consultas. Em seguida, associe cada regra às VPCs para as quais você deseja encaminhar consultas de DNS para sua rede. Por exemplo, crie regras separadas para exemplo.com, exemplo.org e exemplo.net. Em seguida, você pode associar as regras às VPCs em uma AWS região em qualquer combinação.

Encaminhamento de consultas de amazonaws.com para sua rede

O nome de domínio amazonaws.com é o nome de domínio público para AWS recursos como instâncias EC2 e buckets S3. Se quiser encaminhar consultas de amazonaws.com à sua rede, crie uma regra, especifique amazonaws.com para o nome de domínio e especifique Forward (Encaminhar) para o tipo de regra.

> **Note**
>
> O Resolver não encaminha automaticamente consultas de DNS de alguns subdomínios amazonaws.com, mesmo se você criar uma regra de encaminhamento para amazonaws.com. Para ter mais informações, consulte Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas. Para obter informações sobre como substituir esse comportamento, consulte "Encaminhamento de todas as consultas para sua rede" logo a seguir.

Encaminhamento de todas as consultas para sua rede

Se quiser encaminhar todas as consultas à sua rede, crie uma regra, especifique “.” (ponto) para o nome de domínio e associe a regra com as VPCs para as quais quer encaminhar todas as consultas de DNS à sua rede. O resolvedor ainda não encaminha todas as consultas de DNS para sua rede porque usar um resolvedor de DNS externo AWS interromperia algumas funcionalidades. Por exemplo, alguns nomes de AWS domínio internos têm intervalos de endereços IP internos que não podem ser acessados de fora AWS. Para obter uma lista dos nomes de domínio para os quais as consultas não são encaminhadas à sua rede ao criar uma regra para ".", consulte Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas.

Porém, regras de sistema automaticamente definidas para DNS reverso podem ser desabilitadas, permitindo que a regra “.” encaminhe todas as consultas de DNS reverso à sua rede. Para saber mais sobre como desativar as regras definidas automaticamente, consulte Regras de encaminhamento para consultas DNS reversas no Resolver.

Se quiser tentar encaminhar consultas de DNS de todos os nomes de domínio para sua rede, incluindo os nomes de domínio que estão excluídos do encaminhamento por padrão, crie uma regra "." e execute uma das seguintes ações:

- Defina o sinalizador `enableDnsHostnames` da VPC para `false`
- Crie regras para os nomes de domínio que estão listados em Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas

> **Important**
>
> Se você encaminhar todos os nomes de domínio para sua rede, incluindo os nomes de domínio excluídos pelo Resolver ao criar uma regra “.”, alguns recursos poderão parar de funcionar.

Como o Resolver determina se o nome do domínio em uma consulta corresponde a uma regra

O Route 53 Resolver compara o nome de domínio na consulta de DNS com o nome de domínio nas regras associadas à VPC a partir da qual a consulta se originou. O Resolver considera os nomes de domínio para corresponder nos seguintes casos:

- Os nomes de domínio correspondem exatamente
- O nome de domínio na consulta é um subdomínio do nome de domínio na regra

Por exemplo, se o nome de domínio na regra for acme.example.com, o Resolver considerará os seguintes nomes de domínio em uma consulta de DNS para correspondência:

- acme.example.com
- zenith.acme.example.com

Os nome de domínio a seguir não correspondem:

- exemplo.com
- nadir.exemplo.com

Se o nome de domínio em uma consulta corresponder ao nome de domínio em mais de uma regra (como example.com e www.example.com), o Resolver direcionará consultas de DNS de saída usando a regra que contém o nome de domínio mais específico (www.example.com).

Como o Resolver determina para onde encaminhar consultas de DNS

Quando uma aplicação é executada em uma instância do EC2 em uma VPC que envia uma consulta de DNS, o Route 53 Resolver executa as seguintes etapas:

1. O resolvedor verifica os nomes de domínio em regras.

   Se o nome de domínio em uma consulta corresponder ao nome de domínio em uma regra, o Resolver encaminhará a consulta ao endereço IP especificado durante a criação do endpoint de saída. Em seguida, o endpoint de saída encaminha a consulta aos endereços IP dos resolvedores na rede, especificados durante a criação da regra.

   Para ter mais informações, consulte Como o Resolver determina se o nome do domínio em uma consulta corresponde a uma regra.
2. O endpoint do Resolver encaminhará as consultas de DNS com base nas configurações da regra ".".

   Se o nome de domínio em uma consulta não corresponder ao nome do domínio em qualquer outra regra, o Resolver encaminhará a consulta com base nas configurações da regra de "." (ponto) autodefinida. A regra de pontos se aplica a todos os nomes de domínio, exceto alguns nomes de domínio AWS internos e nomes de registros em zonas hospedadas privadas. Essa regra faz com que o Resolver encaminhe consultas de DNS para servidores de nome públicos se os nomes de domínio em consultas não corresponderem a nenhum dos nomes das regras

de encaminhamento personalizadas. Se quiser encaminhar todas as consultas aos resolvedores de DNS em sua rede, crie uma regra de encaminhamento personalizada, especifique "." para o nome de domínio, especifique Forwarding (Encaminhamento) para Type (Tipo) e especifique os endereços IP desses resolvedores.

3. O Resolver retorna a resposta à aplicação que enviou a consulta.

Usar regras em várias regiões

O Route 53 Resolver é um serviço regional, portanto, os objetos que você cria em uma AWS região estão disponíveis somente nessa região. Para usar a mesma regra em mais de uma Região, é necessário criar a regra em cada Região.

A AWS conta que criou uma regra pode compartilhar a regra com outras AWS contas. Para ter mais informações, consulte Compartilhamento de regras do Resolvedor com outras AWS contas e uso de regras compartilhadas.

Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas

O resolvedor cria automaticamente regras de sistema autodefinidas que definem como as consultas de domínios selecionados são resolvidas por padrão:

- Para zonas hospedadas privadas e para nomes de domínio específicos do Amazon EC2 (como compute.amazonaws.com e compute.internal), regras autodefinidas garantem que suas zonas hospedadas privadas e instâncias do EC2 continuem a ser resolvidas, se você criar regras de encaminhamento condicional para nomes de domínio menos específicos, como “.” (ponto) ou “com”.
- Para nomes de domínio publicamente reservados (como localhost and 10.in-addr.arpa), as melhores práticas de DNS recomendam que as consultas sejam respondidas localmente em vez de serem encaminhadas aos servidores de nome públicos. Consulte RFC 6303, zonas de DNS atendidas localmente.

> **Note**
>
> Se você criar uma regra de encaminhamento condicional para "." (ponto) ou "com", recomendamos que também crie uma regra de sistema para amazonaws.com. (As regras de sistema fazem com que o Resolver resolva localmente as consultas de DNS para domínios e subdomínios específicos.) A criação dessa regra de sistema melhora a performance,

reduz o número de consultas que são encaminhadas para sua rede e reduz os encargos do Resolver.

Se desejar substituir uma regra autodefinida, você poderá criar uma regra de encaminhamento condicional para o mesmo nome de domínio.

Também é possível desabilitar algumas das regras definidas automaticamente. Para ter mais informações, consulte Regras de encaminhamento para consultas DNS reversas no Resolver.

O resolvedor cria as seguintes regras autodefinidas.

Regras para zonas hospedadas privadas

Para cada zona hospedada privada associada a uma VPC, o Resolver cria uma regra e associa ela a uma VPC. Se você associar a zona hospedada privada a várias VPCs, o Resolver associará a regra às mesmas VPCs.

A regra tem o tipo Forward (Encaminhar).

Regras para vários nomes de domínio AWS internos

Todas as regras para os nomes de domínio internos nesta seção são do tipo Forward (Encaminhar). O Resolver encaminha consultas de DNS para esses nomes de domínio aos servidores de nome confiáveis da VPC.

> **Note**
>
> O Resolver cria a maioria dessas regras quando você define o sinalizador `enableDnsHostnames` de uma VPC para `true`. O Resolver cria as regras mesmo se você não estiver usando endpoints do Resolver.

O Resolver cria as seguintes regras autodefinidas e associa elas a uma VPC ao definir o sinalizador `enableDnsHostnames` da VPC como `true`:

- *Region-name*.compute.internal, por exemplo, eu-west-1.compute.internal. A região us-east-1 não usa este nome de domínio.
- *Region-name*.compute.*amazon-domain-name*, por exemplo, eu-west-1.compute.amazonaws.com ou cn-north-1.compute.amazonaws.com.cn. A região us-east-1 não usa este nome de domínio.

- ec2.internal. Somente a região us-east-1 usa este nome de domínio.
- compute-1.internal. Somente a região us-east-1 usa este nome de domínio.
- compute-1.amazonaws.com. Somente a região us-east-1 usa este nome de domínio.

As regras autodefinidas a seguir se referem à pesquisa de DNS reversa para as regras criadas pelo Resolver ao definir o sinalizador `enableDnsHostnames` para a VPC como `true`.

- 10.in-addr.arpa
- 16.172.in-addr.arpa por meio de 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa
- Regras para cada um dos intervalos CIDR da VPC. Por exemplo, se uma VPC tiver um intervalo CIDR de 10.0.0.0/23, o Resolver criará as seguintes regras:
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

As regras autodefinidas a seguir, para domínios relacionados ao host local, também são criadas e associadas a uma VPC ao definir o sinalizador `enableDnsHostnames` da VPC como `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

O Resolver cria as seguintes regras autodefinidas e associa elas à sua VPC ao conectar a VPC a outra VPC por meio de gateway de trânsito ou emparelhamento de VPC e com suporte a DNS habilitado:

- A pesquisa de DNS reversa para os intervalos de endereços IP da VPC pareada, por exemplo, 0.192.in-addr.arpa

  Se você adicionar um bloco CIDR IPv4 a uma VPC, o Resolver adicionará uma regra autodefinida para o novo intervalo de endereços IP.
- Se a outra VPC estiver em outra Região, os seguintes nomes de domínio:
  - *`Region-name`*.compute.internal. A região us-east-1 não usa este nome de domínio.
  - *`Region-name`*.compute.*`amazon-domain-name`*. A região us-east-1 não usa este nome de domínio.

- ec2.internal. Somente a região us-east-1 usa este nome de domínio.
- compute-1.amazonaws.com. Somente a região us-east-1 usa este nome de domínio.

Uma regra para todos os outros domínios

O Resolver cria uma regra “.” (ponto) que se aplica a todos os nomes de domínio que não foram especificados anteriormente neste tópico. A regra “.” é do tipo Recursive (Recursiva), o que significa que a regra faz com que o Resolver atue como um resolvedor recursivo.

Considerações ao criar endpoints de entrada e de saída

Antes de criar endpoints do Resolver de entrada e saída em uma AWS região, considere os seguintes problemas.

Tópicos

Número de endpoints de entrada e saída em cada região da

Quando você deseja integrar o DNS para as VPCs em uma AWS região com o DNS para sua rede, você normalmente precisa de um endpoint de entrada do Resolver (para consultas de DNS que você está encaminhando para suas VPCs) e um endpoint de saída (para consultas que você está encaminhando de suas VPCs para sua rede). Você pode criar vários endpoints de entrada e de saída, mas um endpoint de entrada ou de saída é suficiente para processar as consultas de DNS em qualquer direção respectiva. Observe o seguinte:

- Para cada endpoint do Resolver, você especifica dois ou mais endereços IP em diferentes zonas de disponibilidade. Cada endereço IP em um endpoint pode lidar com um grande número de

consultas de DNS por segundo. (Para saber o atual número máximo de consultas por segundo por endereço IP em um endpoint, consulte Cotas no Route 53 Resolver.) Se precisa que o Resolver processe mais consultas, você pode adicionar mais endereços IP ao seu endpoint existente em vez de adicionar outro endpoint.

- A definição de preço do Resolver é baseada no número de endereços IP em seus endpoints e no número de consultas de DNS que o endpoint processa. Cada endpoint inclui um mínimo de dois endereços IP. Para obter mais informações sobre o preço do Resolver, consulte Preço do Amazon Route 53.
- Cada regra especifica o endpoint de saída a partir do qual as consultas de DNS são encaminhadas. Se criar vários endpoints de saída em uma região da AWS e quiser associar algumas ou todas as regras do Resolver a cada VPC, você precisará criar várias cópias dessas regras.

Uso da mesma VPC para endpoints de entrada e de saída

Você pode criar endpoints de entrada e de saída na mesma VPC ou em diferentes VPCs na mesma região.

Para ter mais informações, consulte Práticas recomendadas do Amazon Route 53.

Endpoints de entrada e zonas hospedadas privadas

Se você quiser que o Resolver resolva consultas de DNS de entrada usando registros em uma zona hospedada privada, associe a zona hospedada privada à VPC na qual você criou o endpoint de entrada. Para obter informações sobre como associar zonas hospedadas privadas a VPCs, consulte Trabalhar com zonas hospedadas privadas.

Emparelhamento de VPC

Você pode usar qualquer VPC em uma AWS região para um endpoint de entrada ou saída, independentemente de a VPC escolhida estar emparelhada com outras VPCs. Para obter mais informações, consulte Emparelhamento de Amazon Virtual Private Cloud VPC.

Endereços IP em sub-redes compartilhadas

Ao criar um endpoint de entrada ou de saída, é possível especificar um endereço IP em uma sub-rede compartilhada somente se a conta atual criou a VPC. Se outra conta criar uma VPC e compartilhar uma sub-rede na VPC com sua conta, não será possível especificar um endereço IP

nessa sub-rede. Para obter mais informações sobre sub-redes compartilhadas, consulte Como trabalhar com VPCs compartilhadas no Manual do usuário da Amazon VPC.

Conexão entre a rede e as VPCs nas quais você cria endpoints

Você deve ter uma das seguintes conexões entre a rede e as VPCs nas quais cria endpoints:

- Endpoints de entrada: é necessário configurar uma conexão do AWS Direct Connect ou uma conexão VPN entre a rede e cada VPC para a qual criou um endpoint de entrada.
- Endpoints de saída: é necessário configurar uma conexão do AWS Direct Connect, uma conexão VPN ou um gateway de Conversão de endereços de rede (NAT) entre a rede e cada VPC para a qual foi criado um endpoint de saída.

Quando compartilha regras, você também compartilha endpoints de saída

Ao criar uma regra, você especifica o endpoint de saída que você quer que o Resolver use para encaminhar consultas de DNS para sua rede. Se você compartilhar a regra com outra AWS conta, também compartilhará indiretamente o endpoint de saída especificado na regra. Se você usou mais de uma AWS conta para criar VPCs em uma AWS região, você pode fazer o seguinte:

- Crie um endpoint de saída na região.
- Crie regras usando uma AWS conta.
- Compartilhe as regras com todas as AWS contas que criaram VPCs na região.

Isso permite que você use um endpoint de saída em uma região para encaminhar consultas de DNS para sua rede a partir de várias VPCs, mesmo que as VPCs tenham sido criadas usando contas diferentes. AWS

Escolher protocolos para os endpoints

Os protocolos dos endpoints determinam como os dados são transmitidos para um endpoint de entrada e de um endpoint de saída. Não é necessário criptografar as consultas ao DNS para tráfego na VPC porque todo fluxo de pacotes na rede é autorizado individualmente de acordo com uma regra para validar a origem e o destino corretos antes de ser transmitido e entregue. A troca arbitrária de informações entre entidades sem a autorização específica da entidade transmissora e da entidade receptora é extremamente improvável. Se um pacote for roteado para um destino sem que haja uma regra correspondente, ele será descartado. Para obter mais informações, consulte Recursos da VPC.

Os protocolos disponíveis são:

- Do53: DNS pela porta 53. Os dados são retransmitidos usando o Route 53 Resolver sem criptografia adicional. Embora os dados não possam ser lidos por terceiros, eles podem ser visualizados nas AWS redes. Usa UDP ou TCP para enviar os pacotes. O Do53 é usado principalmente para tráfego nas Amazon VPCs e entre elas.
- DoH: os dados são transmitidos em uma sessão HTTPS criptografada. O DoH adiciona mais um nível de segurança em que os dados não podem ser descriptografados por usuários não autorizados e não podem ser lidos por ninguém, a não ser pelo destinatário pretendido.
- DoH-FIPS: os dados são transmitidos em uma sessão HTTPS criptografada conforme o padrão criptográfico FIPS 140-2. Compatível apenas com endpoints de entrada. Para obter mais informações, consulte FIPS PUB 140-2.

Para um endpoint de entrada, você pode aplicar os protocolos da seguinte maneira:

- Do53 e DoH combinados.
- Do53 e DoH-FIPS combinados.
- D53 sozinho.
- DoH sozinho.
- DoH-FIPS sozinho.
- Nenhum, o que é tratado como Do53.

Para um endpoint de saída, você pode aplicar os protocolos da seguinte maneira:

- Do53 e DoH combinados.
- D53 sozinho.
- DoH sozinho.
- Nenhum, o que é tratado como Do53.

Consulte também Valores especificados ao criar ou editar endpoints de entrada e Valores especificados ao criar ou editar endpoints de saída.

Como usar o resolvedor em VPCs que são configuradas para locação de instâncias dedicadas

Quando você cria um endpoint do Resolver, não é possível especificar uma VPC que tenha o atributo de locação de instância definido como `dedicated`. O Resolver não é executado no hardware de locação única.

Você ainda pode usar o Resolver para resolver consultas de DNS que se originam em uma VPC. Crie pelo menos uma VPC com o atributo de locação de instância definido como `default` e especifique essa VPC ao criar endpoints de entrada e saída.

Quando você cria uma regra de encaminhamento, pode associá-la a qualquer VPC, independentemente da configuração do atributo de locação de instância.

Disponibilidade e escalabilidade do Route 53 Resolver

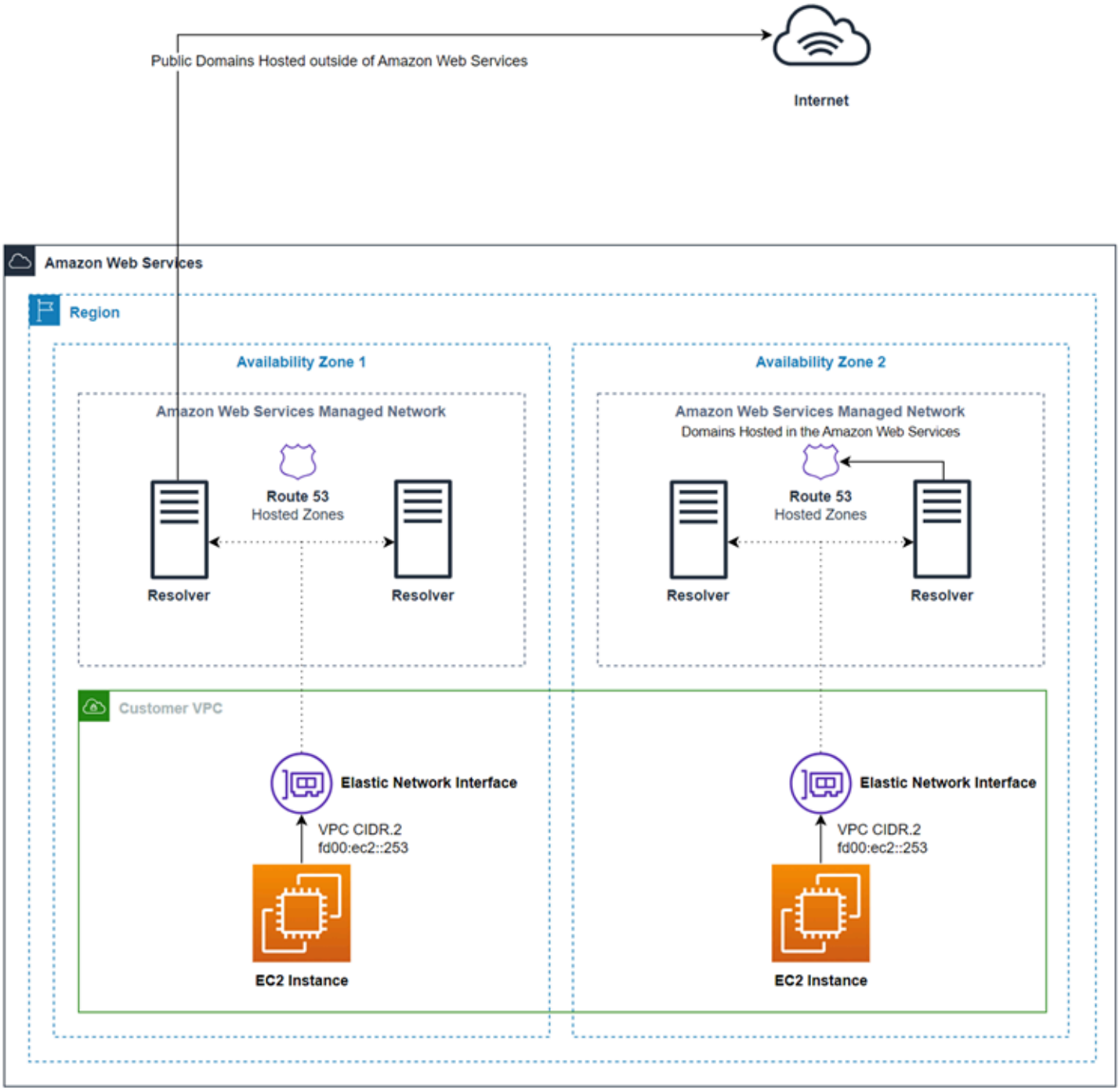
Amazon Route 53 Resolver, executado no endereço CIDR + 2 da Amazon VPC e fd00:ec2: :253, está disponível por padrão em todas as VPCs e responde recursivamente às consultas de DNS para registros públicos, nomes DNS específicos do Amazon VPC e zonas hospedadas privadas do Route 53. Há dois componentes altamente disponíveis, transparentes para os usuários, que compõem o Route 53 Resolver: o serviço Nitro Resolver e a frota Zonal Resolver. O Nitro Resolver Service é um serviço executado na placa Nitro em instâncias Nitro e em Dom0 em instâncias de gerações mais antigas e consome pacotes endereçados ao Route 53 Resolver localmente no servidor host. Para obter mais informações, consulte O design de segurança do sistema AWS Nitro.

O serviço Nitro Resolver carrega um cache local que pode ajudar a reduzir a latência respondendo a consultas repetidas feitas por uma instância em um curto período de tempo. Quando o serviço Nitro Resolver recebe uma consulta para a qual não tem uma resposta em cache, ele encaminha a consulta para a frota do Zonal Resolver, uma frota de resolvedores altamente disponível, normalmente na mesma zona de disponibilidade da instância. Quando há falhas no tratamento de consultas de servidores de nomes upstream ou outros componentes no caminho, o serviço Nitro Resolver geralmente consegue lidar com essas falhas de forma transparente, sem afetar as cargas de trabalho em execução na instância. Além disso, se o Resolvedor encontrar tempos limite de consulta, conexões recusadas ou SERVFAILS dos servidores de nomes do domínio, ele poderá responder com uma resposta em cache além do valor de Time-To-Live (TTL) para melhorar a disponibilidade. As consultas entre o serviço Nitro Resolver e a frota do Zonal Resolver são restritas a uma rede rigidamente controlada fora da VPC do cliente, que é inacessível aos clientes e sujeita

a controles de segurança rigorosos. Ao lidar com consultas entre o serviço Nitro Resolver e a frota do Zonal Resolver fora da VPC, os clientes são impedidos de interceptar consultas de DNS dentro da VPC. As consultas destinadas a servidores de nomes externos AWS percorrerão a Internet pública, originadas de endereços IP públicos pertencentes à frota do Zonal Resolver. Atualmente, não oferecemos suporte ao atributo eDNS0-Client Subnet, o que significa que todas as consultas destinadas a servidores de nomes DNS públicos não incluem informações sobre o endereço IP do cliente de origem.

O serviço Nitro Resolver faz parte dos serviços Link-Local na instância. Os serviços Link-Local incluem o Route 53 Resolver, o Amazon Time Service (NTP), o Instance Metadata Service (IMDS) e o Windows Licensing Service (para instâncias do Windows). Esses serviços escalam com cada interface de rede elástica que você cria em sua VPC, e cada interface de rede permite 1024 pacotes por segundo (PPS) destinados aos serviços Link-Local. Pacotes que excedem esse limite são rejeitados. Você pode determinar se excedeu esse limite a partir do `linklocal_allowance_exceeded` valor retornado pelo ethtool. Para obter mais informações sobre o ethtool, consulte Monitore o desempenho da rede para sua instância do Amazon EC2 no Guia do usuário do Amazon EC2. Essa métrica também pode ser reportada às CloudWatch métricas pelo CloudWatch agente. Como o Route 53 Resolver é implementado por interface de rede, ele se expande e se torna mais confiável à medida que você adiciona mais instâncias em mais zonas de disponibilidade. Não há limite agregado por VPC no número de consultas, portanto, o Route 53 Resolver pode ser escalado dentro dos limites de uma VPC, que é inerentemente baseada no uso do endereço de rede (NAU). Para obter mais informações, consulte Uso de endereços de rede para sua VPC no Guia do usuário da Amazon Virtual Private Cloud.

O diagrama a seguir mostra uma visão geral de como o Route 53 Resolver resolve consultas de DNS nas zonas de disponibilidade.



Conceitos básicos do Route 53 Resolver

O console do Route 53 Resolver inclui um assistente que orienta você durante as etapas a seguir para começar a usar o Resolver:

- Crie endpoints: de entrada, de saída ou ambos.

- Para endpoints de saída, crie uma ou mais regras de encaminhamento, que especificam os nomes de domínio para os quais você deseja rotear consultas de DNS para sua rede.
- Se você criou um endpoint de saída, escolha a VPC com a qual deseja associar as regras.

Para configurar o Route 53 Resolver usando o assistente

1. Faça login AWS Management Console e abra o console do Resolver em https://console.aws.amazon.com/route53resolver/.
2. Na página Welcome to Route 53 Resolver (Bem-vindo ao Route 53 Resolver), selecioneConfigure endpoints (Configurar endpoints).
3. Na barra de navegação, escolha a Região onde deseja criar um endpoint de resolvedor.
4. Em Basic configuration (Configuração básica), escolha a direção em que deseja encaminhar as consultas de DNS:

   - Inbound and outbound (Entrada e saída): o assistente o orienta pelas configurações que permitem encaminhar consultas de DNS de resolvedores da rede para o Resolver em uma VPC e encaminhar consultas especificadas (como example.com ou example.net) de uma VPC para resolvedores da rede.
   - Inbound only (Somente entrada): o assistente o orienta pelas configurações que permitem encaminhar consultas de DNS de resolvedores da rede para o Resolver em uma VPC.
   - Outbound only (Somente saída): o assistente te orienta pelas configurações que permitem encaminhar consultas especificadas de uma VPC para resolvedores da rede.
5. Selecione Next (Próximo).
6. Se você escolheu Inbound and outbound (Entrada e saída) ou Inbound only (Somente entrada), insira os valores aplicáveis para configurar um endpoint de entrada. Em seguida, passe para a etapa 7. Para ter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada.

   Se você escolher Outbound only (Somente saída), pule para a etapa 7.
7. Insira os valores aplicáveis para configurar um endpoint de saída. Para ter mais informações, consulte Valores especificados ao criar ou editar endpoints de saída.
8. Se você escolheu Inbound and outbound (Entrada e saída) ou Outbound only (Somente saída), insira os valores aplicáveis para criar uma regra. Para ter mais informações, consulte Valores especificados ao criar ou editar regras.

9. Na página Review and create (Revisar e criar), confirme se as configurações especificadas nas páginas anteriores estão corretas. Se necessário, escolha Edit (Editar) na seção aplicável e atualize as configurações. Quando estiver satisfeito com as configurações, clique em Submit (Enviar).

   > **Note**
   >
   > A criação de um endpoint de saída leva um ou dois minutos. Não é possível criar outro endpoint de saída antes que o primeiro seja criado.

10. Se quiser criar mais regras, consulte Gerenciamento de regras de encaminhamento.
11. Se você criou um endpoint de entrada, configure resolvedores de DNS na rede para encaminhar consultas de DNS aplicáveis aos endereços IP do endpoint de entrada. Para obter mais informações, consulte a documentação de seu aplicativo de DNS.

Encaminhamento de consultas de DNS de entrada para as VPCs

Para encaminhar consultas de DNS de sua rede para o Resolver, crie um endpoint de entrada. Um endpoint de entrada especifica os endereços IP (do intervalo de endereços IP disponíveis para sua VPC) para os quais você deseja que os resolvedores de DNS em sua rede encaminhem consultas de DNS. Esses endereços IP não são endereços IP públicos. Portanto, para cada endpoint de entrada, você precisa conectar sua VPC à sua rede usando uma AWS Direct Connect conexão ou uma conexão VPN.

Tópicos

Configurar o encaminhamento de entrada

Para criar um endpoint de entrada, execute o seguinte procedimento.

Para criar um endpoint de entrada

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Inbound endpoints (Endpoints de entrada).

3. Na barra de navegação, escolha a Região onde deseja criar um endpoint de entrada.
4. Escolha Create inbound endpoint (Criar endpoint de entrada).
5. Insira os valores aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada.
6. Escolha Criar.
7. Configure os resolvedores de DNS na rede para encaminhar consultas de DNS aplicáveis aos endereços IP do endpoint de entrada. Para obter mais informações, consulte a documentação de seu aplicativo de DNS.

Valores especificados ao criar ou editar endpoints de entrada

Ao criar ou editar um endpoint de entrada, especifique os seguintes valores:

ID do Outpost

Se você estiver criando o endpoint para um resolvedor em uma AWS Outposts VPC, esse é AWS Outposts o ID.

Nome do endpoint

Um nome amigável que permite encontrar facilmente um endpoint de entrada no painel.

VPC na Região region-name

Todas as consultas de DNS de entrada da rede passam por essa VPC em direção do Resolver.

Grupo de segurança para este endpoint

O ID de um ou mais grupos de segurança que deseja usar para controlar o acesso a essa VPC. O grupo de segurança especificado deve incluir uma ou mais regras de entrada. As regras de entrada devem permitir o acesso TCP e UDP na porta 53. Não é possível alterar esse valor depois de criar o endpoint.

Algumas regras do grupo de segurança farão com que sua conexão seja rastreada e o máximo geral de consultas por segundo por endereço IP para um endpoint de entrada pode ser tão baixo quanto 1500. Para evitar o rastreamento de conexão causado por um grupo de segurança, consulte Conexões não rastreadas.

> **Note**
>
> Para adicionar vários grupos de segurança, use o AWS CLI comando`create-resolver-endpoint`. Para obter mais informações, consulte create-resolver-endpoint

Para mais informações, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Tipo de endpoint

O tipo de endpoint pode ser endereços IP IPv4, IPv6 ou de pilha dupla. Para um endpoint de pilha dupla, o endpoint terá endereços IPv4 e IPv6 para os quais o resolver de DNS na rede pode encaminhar a consulta ao DNS.

> **Note**
>
> Por motivos de segurança, estamos negando o acesso direto ao tráfego IPv6 da Internet pública para todos os endereços IP de pilha dupla e IPv6.

Endereços IP

Os endereços IP para os quais deseja que os resolvedores de DNS encaminhem as consultas de DNS. Exigimos que você especifique um mínimo de dois endereços IP para redundância. Observe o seguinte:

Várias zonas de disponibilidade

É recomendável especificar endereços IP em pelo menos duas zonas de disponibilidade. Opcionalmente, você pode especificar endereços IP adicionais nessas ou em outras zonas de disponibilidade.

Endereços IP e interfaces de rede elástica da Amazon VPC

Para cada combinação de zona de disponibilidade, sub-rede e endereço IP que você especificar, o Resolver criará uma interface de rede elástica da Amazon VPC. Para saber o atual número máximo de consultas de DNS por segundo por endereço IP em um endpoint, consulte Cotas no Route 53 Resolver. Para obter informações sobre os preços de cada interface de rede elástica, consulte “Amazon Route 53”, na página de preços do Amazon Route 53.

> **Note**
>
> O endpoint do Resolver tem um endereço IP privado. Esses endereços IP não mudarão ao longo da vida útil de um endpoint.

Para cada endereço IP, especifique os valores a seguir. Cada endereço IP deve estar em uma zona de disponibilidade na VPC especificada em VPC na região region-name (nome da região).

Availability Zone (zona de disponibilidade)

A zona de disponibilidade pelas quais você deseja que as consultas de DNS passem a caminho de sua VPC. A zona de disponibilidade especificada deve ser configurada com uma sub-rede.

Sub-rede

A sub-rede que contém os endereços IP que você deseja atribuir aos ENIs do endpoint do Resolver. Esses são os endereços para os quais você enviará consultas de DNS. A sub-rede deve ter um endereço IP disponível.

O endereço IP da sub-rede deve corresponder ao Tipo de endpoint.

Endereço IP

Um endereço IP para o qual você deseja encaminhar consultas de DNS.

Decida se você quer que o Resolver escolha um endereço IP para você entre os endereços IP disponíveis na sub-rede especificada ou se quer especificar você mesmo o endereço IP.

Se você optar por especificar o endereço IP por conta própria, insira um endereço IPv4 ou IPv6, ou ambos.

Protocolos

O protocolo do endpoint determina como os dados são transmitidos ao endpoint de entrada. Escolha um ou mais protocolos dependendo do nível de segurança necessário.

- Do53: (padrão) os dados são retransmitidos usando o Route 53 Resolver sem criptografia adicional. Embora os dados não possam ser lidos por terceiros, eles podem ser visualizados nas redes da AWS .
- DoH: os dados são transmitidos em uma sessão HTTPS criptografada. O DoH adiciona mais um nível de segurança em que os dados não podem ser descriptografados por usuários não autorizados e não podem ser lidos por ninguém, a não ser pelo destinatário pretendido.

- DoH-FIPS: os dados são transmitidos em uma sessão HTTPS criptografada conforme o padrão criptográfico FIPS 140-2. Compatível apenas com endpoints de entrada. Para obter mais informações, consulte FIPS PUB 140-2.

Para um endpoint de entrada, você pode aplicar os protocolos da seguinte maneira:

- Do53 e DoH combinados.
- Do53 e DoH-FIPS combinados.
- D53 sozinho.
- DoH sozinho.
- DoH-FIPS sozinho.
- Nenhum, o que é tratado como Do53.

> **Important**
>
> Você não pode alterar o protocolo de um endpoint de entrada diretamente do Do53 sozinho para o DoH sozinho ou para o DoH-FIPS. Isso evita uma interrupção repentina no tráfego de entrada que usa o Do53. Para mudar o protocolo do Do53 para o DoH ou para o DoH-FIPS, você deve primeiro habilitar ambos o Do53 e o DoH ou o Do53 e o DoH-FIPS para garantir que todo o tráfego de entrada passe a usar o protocolo DoH ou DoH-FIPS antes que o Do53 seja removido.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Encaminhar consultas de DNS de saída para a rede

Para encaminhar consultas de DNS originadas em instâncias do Amazon EC2 em uma ou mais VPCs para a rede, crie um endpoint de saída e uma ou mais regras:

Endpoint de saída

Para encaminhar consultas de DNS das VPCs para a rede, crie um endpoint de saída. Um endpoint de saída especifica os endereços IP dos quais as consultas se originam. Esses

endereços IP, que você escolhe no intervalo de endereços IP disponíveis para sua VPC, não são públicos. Isso significa que, para cada endpoint de saída, é necessário conectar a VPC à sua rede usando a conexão do AWS Direct Connect , uma conexão VPC ou um gateway de Conversão de endereços de rede (NAT). Observe que é possível usar o mesmo endpoint de saída para várias VPCs na mesma região ou criar vários endpoints de saída. Se quiser que seu endpoint de saída use DNS64, habilite o DNS64 usando a Amazon Virtual Private Cloud. Para obter mais informações, consulte DNS64 e NAT64, no Guia do usuário da Amazon VPC.

O IP de destino da regra do Resolvedor do Route 53 é escolhido aleatoriamente pelo Resolver e não há preferência em escolher um IP de destino específico em detrimento do outro. Se um IP de destino não responder à solicitação de DNS encaminhada, o Resolvedor tentará novamente acessar um endereço IP aleatório entre os IPs de destino.

Regras

Para especificar nomes de domínio das consultas que você deseja encaminhar para os resolvedores de DNS na rede, crie uma ou mais regras. Cada regra especifica um nome de domínio. Em seguida, associe as regras às VPCs para as quais você deseja encaminhar consultas para sua rede.

Para obter mais informações, consulte os tópicos a seguir.

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

Configurar o encaminhamento de saída

Para configurar o Resolver a fim de encaminhar consultas de DNS originadas em sua VPC para a rede, execute os procedimentos a seguir.

> **Important**
>
> Depois de criar um endpoint de saída, é necessário criar uma ou mais regras e associá-las a uma ou mais VPCs. As regras especificam os nomes de domínio das consultas de DNS que você deseja encaminhar para sua rede.

Para criar um endpoint de saída

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Outbound endpoints (Endpoints de saída).
3. Na barra de navegação, escolha a Região onde deseja criar um endpoint de saída.
4. Escolha Create outbound endpoint (Criar endpoint de saída).
5. Insira os valores aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar endpoints de saída.
6. Escolha Criar.

> **Note**
>
> A criação de um endpoint de saída leva um ou dois minutos. Não é possível criar outro endpoint de saída antes que o primeiro seja criado.

7. Crie uma ou mais regras para especificar os nomes de domínio das consultas de DNS que deseja encaminhar à sua rede. Para obter mais informações, consulte o próximo procedimento.

Para criar uma ou mais regras de encaminhamento, execute o procedimento a seguir.

Para criar regras de encaminhamento e associá-las a uma ou mais VPCs

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a região onde você quer criar a regra.
4. Escolha Criar Regra.
5. Insira os valores aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar regras.
6. Escolha Salvar.
7. Para adicionar outra regra, repita as etapas de 4 a 6.

Valores especificados ao criar ou editar endpoints de saída

Ao criar ou editar um endpoint de saída, especifique os seguintes valores:

ID do Outpost

Se você estiver criando o endpoint para um resolvedor em uma AWS Outposts VPC, esse é AWS Outposts o ID.

Nome do endpoint

Um nome amigável que permite encontrar facilmente um endpoint de saída no painel.

VPC na Região region-name

Todas as consultas de DNS de saída fluirão por esta VPC a caminho de sua rede.

Grupo de segurança para este endpoint

O ID de um ou mais grupos de segurança que deseja usar para controlar o acesso a essa VPC. O grupo de segurança especificado deve incluir uma ou mais regras de saída. As regras de saída devem permitir o acesso TCP e UDP na porta que você está usando para consultas de DNS na rede. Não é possível alterar esse valor depois de criar um endpoint.

Algumas regras do grupo de segurança farão com que sua conexão seja rastreada e potencialmente afetarão o máximo de consultas por segundo do endpoint de saída para o servidor de nomes de destino. Para evitar o rastreamento de conexão causado por um grupo de segurança, consulte Conexões não rastreadas.

Para mais informações, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Tipo de endpoint

O tipo de endpoint pode ser endereços IP IPv4, IPv6 ou de pilha dupla. Para um endpoint de pilha dupla, o endpoint terá endereços IPv4 e IPv6 para os quais o resolver de DNS na rede pode encaminhar a consulta ao DNS.

> **Note**
>
> Por motivos de segurança, estamos negando acesso direto ao tráfego IPv6 à Internet pública para todos os endereços IP de pilha dupla e IPv6.

Endereços IP

Os endereços IP da VPC para os quais você quer que o Resolver encaminhe consultas de DNS em direção dos resolvedores em sua rede. Esses não são os endereços IP dos resolvedores de DNS em sua rede. Especifique esses endereços IP de resolvedor ao criar as regras que você associa a uma ou mais VPCs. Exigimos que você especifique um mínimo de dois endereços IP para redundância.

> **Note**
>
> O endpoint do Resolver tem um endereço IP privado. Esses endereços IP não mudarão ao longo da vida útil de um endpoint.

Observe o seguinte:

Várias zonas de disponibilidade

É recomendável especificar endereços IP em pelo menos duas zonas de disponibilidade. Opcionalmente, você pode especificar endereços IP adicionais nessas ou em outras zonas de disponibilidade.

Endereços IP e interfaces de rede elástica da Amazon VPC

Para cada combinação de zona de disponibilidade, sub-rede e endereço IP que você especificar, o Resolver criará uma interface de rede elástica da Amazon VPC. Para saber o atual número máximo de consultas de DNS por segundo por endereço IP em um endpoint, consulte Cotas no Route 53 Resolver. Para obter informações sobre os preços de cada interface de rede elástica, consulte “Amazon Route 53”, na página de preços do Amazon Route 53.

Ordem dos endereços IP

É possível especificar endereços IP em qualquer ordem. Ao encaminhar consultas DNS, o Resolver não escolhe endereços IP com base na ordem em que os endereços IP estão listados.

Para cada endereço IP, especifique os valores a seguir. Cada endereço IP deve estar em uma zona de disponibilidade na VPC especificada em VPC na região region-name (nome da região).

Availability Zone (zona de disponibilidade)

A zona de disponibilidade pela qual você deseja que as consultas de DNS passem a caminho de sua rede. A zona de disponibilidade especificada deve ser configurada com uma sub-rede.

Sub-rede

A sub-rede que contém o endereço IP do qual você deseja que as consultas de DNS sejam originadas a caminho de sua rede. A sub-rede deve ter um endereço IP disponível.

O endereço IP da sub-rede deve corresponder ao Tipo de endpoint.

Endereço IP

O endereço IP do qual você deseja que as consultas de DNS sejam originadas a caminho de sua rede.

Decida se você quer que o Resolver escolha um endereço IP para você entre os endereços IP disponíveis na sub-rede especificada ou se quer especificar você mesmo o endereço IP.

Se você optar por especificar o endereço IP sozinho, insira um endereço IPv4 ou IPv6, ou ambos.

Protocolos

O protocolo do endpoint determina como os dados são transmitidos do endpoint de saída. Escolha um ou mais protocolos dependendo do nível de segurança necessário.

- Do53: (padrão) os dados são retransmitidos usando o Route 53 Resolver sem criptografia adicional. Embora os dados não possam ser lidos por terceiros, eles podem ser visualizados nas redes da AWS .
- DoH: os dados são transmitidos em uma sessão HTTPS criptografada. O DoH adiciona mais um nível de segurança em que os dados não podem ser descriptografados por usuários não autorizados e não podem ser lidos por ninguém, a não ser pelo destinatário pretendido.

Para um endpoint de saída, você pode aplicar os protocolos da seguinte maneira:

- Do53 e DoH combinados.
- D53 sozinho.
- DoH sozinho.
- Nenhum, o que é tratado como Do53.

Atualmente, a extensão TLS SNI para as consultas DoH no endpoint de saída não é suportada.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Valores especificados ao criar ou editar regras

Ao criar ou editar uma regra de encaminhamento, especifique os seguintes valores:

Nome da regra

Um nome amigável que permita encontrar facilmente uma regra no painel.

Tipo de regra

Escolha o valor aplicável:

- Forward (Encaminhar): escolha essa opção quando quiser encaminhar consultas de DNS de um nome de domínio especificado para resolvedores em sua rede.
- System (Sistema): escolha essa opção quando quiser que o Resolver substitua seletivamente o comportamento definido em uma regra de encaminhamento. Ao criar uma regra de sistema, o Resolver resolve consultas de DNS de subdomínios especificados que, de outra forma, seriam resolvidas por resolvedores de DNS na rede.

Por padrão, o encaminhamento de regras se aplica a um nome de domínio e todos os seus subdomínios. Se quiser encaminhar consultas de um domínio para um resolvedor na rede, mas não quiser encaminhar as consultas de alguns subdomínios, crie uma regra de sistema para os subdomínios. Por exemplo, se você criar uma regra de encaminhamento para exemplo.com mas não quiser encaminhar consultas para acme.exemplo.com, crie uma regra de sistema e especifique acme.exemplo.com para o nome de domínio.

VPCs que usam esta regra

As VPCs que usam essa regra para encaminhar consultas de DNS para o nome ou nomes de domínio especificados. É possível aplicar uma regra a quantas VPCs você quiser.

Nome de domínio

As consultas de DNS desse nome de domínio são encaminhadas para os endereços IP especificados em Target IP addresses (Endereços IP de destino). Para ter mais informações,

consulte Como o Resolver determina se o nome do domínio em uma consulta corresponde a uma regra.

Endpoint de saída

O Resolver encaminha consultas de DNS pelo endpoint de saída especificado aqui aos endereços IP especificados em Target IP addresses (Endereços IP de destino).

Endereços IP de destino

Quando uma consulta de DNS corresponde ao nome especificado em Domain name (Nome do domínio), o endpoint de saída encaminha a consulta para os endereços IP especificados aqui. Normalmente, são os endereços IP dos resolvedores de DNS em sua rede.

Target IP addresses (Endereços IP de destino) está disponível apenas quando o valor de Rule type (Tipo de regra) for Forward (Encaminhar).

Especifique os endereços IPv4 ou IPv6 e os protocolos que você deseja usar para o endpoint.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Essas são as etiquetas AWS Billing and Cost Management que permitem organizar sua AWS fatura. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing .

Gerenciamento de endpoints de entrada

Para gerenciar endpoints de entrada, execute o procedimento aplicável.

Tópicos

- Visualizar e editar endpoints de entrada
- Visualizar o status dos endpoints de entrada
- Excluir endpoints de entrada

Visualizar e editar endpoints de entrada

Para visualizar e editar as configurações de um endpoint de entrada, execute o procedimento a seguir.

Para visualizar e editar as configurações de um endpoint de entrada

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Inbound endpoints (Endpoints de entrada).
3. Na barra de navegação, escolha a Região onde o endpoint de entrada foi criado.
4. Escolha a opção do endpoint que deseja visualizar ou editar as configurações.
5. Escolha View details (Visualizar detalhes) ou Edit (Editar).

   Para obter informações sobre os valores dos endpoints de entrada, consulte Valores especificados ao criar ou editar endpoints de entrada.
6. Se você escolheu Edit (Editar), insira os valores aplicáveis e selecione Save (Salvar).

Visualizar o status dos endpoints de entrada

Para visualizar o status de um endpoint de entrada, realize o procedimento a seguir.

Como exibir o status de um endpoint de entrada

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Inbound endpoints (Endpoints de entrada).
3. Na barra de navegação, escolha a Região onde o endpoint de entrada foi criado. A coluna Status contém um dos seguintes valores:

   Criando

   O Resolver está criando e configurando uma ou mais interfaces de rede da Amazon VPC para esse endpoint.

Operacional

As interfaces de rede da Amazon VPC para esse endpoint estão configuradas corretamente e são capazes de passar consultas de DNS de entrada ou de saída entre a rede e o Resolver.

Atualizando

O resolvedor está associando ou desassociando uma ou mais interfaces de rede com esse endpoint.

Recuperação automática

O Resolver está tentando recuperar uma ou mais interfaces de rede associadas a esse endpoint. Durante o processo de recuperação, o endpoint funciona com capacidade limitada por causa do limite do número de consultas de DNS por endereço IP (por interface de rede). Para obter o limite atual, consulte Cotas no Route 53 Resolver.

Ação necessária

Esse endpoint não é íntegro, e o Resolver não pode recuperá-lo automaticamente. Para resolver o problema, recomendamos que você verifique cada endereço IP associado ao endpoint. Para cada endereço IP que não está disponível, adicione outro endereço IP e exclua o endereço IP que não está disponível. (Um endpoint sempre deve incluir pelo menos dois endereços IP.) Um status de Action needed (Ação necessária) pode ter várias causas. Aqui estão duas causas comuns:

- Uma ou mais interfaces de rede associadas ao endpoint foram excluídas usando a Amazon VPC.
- A interface de rede não pôde ser criada por algum motivo que está fora do controle do Resolver.

Excluindo

O resolvedor está excluindo esse endpoint e as interfaces de rede associadas.

Excluir endpoints de entrada

Para excluir um endpoint de entrada, execute o seguinte procedimento.

> **Important**
>
> Se você excluir um endpoint de entrada, as consultas de DNS da sua rede não serão mais encaminhadas para o Resolver na VPC especificada no endpoint.

Para excluir um endpoint de entrada

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Inbound endpoints (Endpoints de entrada).
3. Na barra de navegação, escolha a Região onde o endpoint de entrada foi criado.
4. Escolha a opção do endpoint que deseja excluir.
5. Escolha Excluir.
6. Para confirmar a exclusão do endpoint, insira o nome do endpoint e escolha Submit (Enviar).

Gerenciamento de endpoints de saída

Para gerenciar endpoints de saída, execute o procedimento aplicável.

Tópicos

- Visualizar e editar endpoints de saída
- Visualizar o status dos endpoints de saída
- Excluir endpoints de saída

Visualizar e editar endpoints de saída

Para visualizar e editar as configurações de um endpoint de saída, execute o procedimento a seguir.

Para visualizar e editar as configurações de um endpoint de saída

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Outbound endpoints (Endpoints de saída).
3. Na barra de navegação, escolha a Região onde o endpoint de saída foi criado.

4. Escolha a opção do endpoint que deseja visualizar ou editar as configurações.
5. Escolha View details (Visualizar detalhes) ou Edit (Editar).

   Para obter informações sobre os valores dos endpoints de saída, consulte Valores especificados ao criar ou editar endpoints de saída.
6. Se você escolheu Edit (Editar), insira os valores aplicáveis e, em seguida, selecione Save (Salvar).

Visualizar o status dos endpoints de saída

Para visualizar o status de um endpoint de saída, realize o procedimento a seguir.

Como visualizar o status de um endpoint de saída

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Outbound endpoints (Endpoints de saída).
3. Na barra de navegação, escolha a Região onde o endpoint de saída foi criado. A coluna Status contém um dos seguintes valores:

   Criando

   O Resolver está criando e configurando uma ou mais interfaces de rede da Amazon VPC para esse endpoint.

   Operacional

   As interfaces de rede da Amazon VPC para esse endpoint estão configuradas corretamente e são capazes de passar consultas de DNS de entrada ou de saída entre a rede e o Resolver.

   Atualizando

   O resolvedor está associando ou desassociando uma ou mais interfaces de rede com esse endpoint.

   Recuperação automática

   O Resolver está tentando recuperar uma ou mais interfaces de rede associadas a esse endpoint. Durante o processo de recuperação, o endpoint funciona com capacidade limitada

por causa do limite do número de consultas de DNS por endereço IP (por interface de rede). Para obter o limite atual, consulte Cotas no Route 53 Resolver.

Ação necessária

Esse endpoint não é íntegro, e o Resolver não pode recuperá-lo automaticamente. Para resolver o problema, recomendamos que você verifique cada endereço IP associado ao endpoint. Para cada endereço IP que não está disponível, adicione outro endereço IP e exclua o endereço IP que não está disponível. (Um endpoint sempre deve incluir pelo menos dois endereços IP.) Um status de Action needed (Ação necessária) pode ter várias causas. Aqui estão duas causas comuns:

- Uma ou mais interfaces de rede associadas ao endpoint foram excluídas usando a Amazon VPC.
- A interface de rede não pôde ser criada por algum motivo que está fora do controle do Resolver.

Excluindo

O resolvedor está excluindo esse endpoint e as interfaces de rede associadas.

Excluir endpoints de saída

Antes de excluir um endpoint, você deve primeiro excluir todas as regras associadas a uma VPC.

Para excluir um endpoint de saída, execute o seguinte procedimento.

> **Important**
>
> Se você excluir um endpoint de saída, o Resolver irá parar de encaminhar consultas de DNS de sua VPC à rede para regras que especificam o endpoint de saída excluído.

Para excluir um endpoint de saída

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Outbound endpoints (Endpoints de saída).
3. Na barra de navegação, escolha a Região onde o endpoint de saída foi criado.
4. Escolha a opção do endpoint que deseja excluir.

5. Escolha Excluir.
6. Para confirmar a exclusão do endpoint, insira o nome do endpoint e, em seguida, escolha Submit (Enviar).

Gerenciamento de regras de encaminhamento

Se quiser que o Resolver encaminhe consultas de nomes de domínio especificados para a rede, crie uma regra de encaminhamento para cada nome de domínio e especifique o nome do domínio para o qual você quer encaminhar consultas.

Tópicos

Visualizar e editar regras de encaminhamento

Para visualizar e editar as configurações de uma regra de encaminhamento, execute o procedimento a seguir.

Para visualizar e editar as configurações de uma regra de encaminhamento

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a Região onde a regra foi criada.
4. Escolha a opção da regra que deseja visualizar ou editar as configurações.
5. Escolha View details (Visualizar detalhes) ou Edit (Editar).

Para obter informações sobre os valores das regras de encaminhamento, consulte Valores especificados ao criar ou editar regras.

6. Se você escolheu Edit (Editar), insira os valores aplicáveis e, em seguida, selecione Save (Salvar).

Criar regras de encaminhamento

Para criar uma ou mais regras de encaminhamento, execute o procedimento a seguir.

Para criar regras de encaminhamento e associá-las a uma ou mais VPCs

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a região onde você quer criar a regra.
4. Escolha Criar Regra.
5. Insira os valores aplicáveis. Para ter mais informações, consulte Valores especificados ao criar ou editar regras.
6. Escolha Salvar.
7. Para adicionar outra regra, repita as etapas de 4 a 6.

Como adicionar regras para pesquisa inversa

Se você precisar controlar pesquisas inversas em sua VPC, você pode adicionar regras ao endpoint do resolvedor de saída.

Para criar a regra de pesquisa inversa

1. Siga as etapas no procedimento anterior, até a etapa 5.
2. Quando você especificar sua regra, insira o registro PTR para o endereço IP ou endereços para os quais você quer uma regra de encaminhamento de pesquisa inversa.

   Por exemplo, se você precisar encaminhar pesquisas para endereços no intervalo 10.0.0.0/23, insira duas regras:

   - 0.0.10.in-addr.arpa

- 1.0.10.in-addr.arpa

  Qualquer endereço IP nessas sub-redes será referenciado como um subdomínio desses registros PTR: por exemplo, 10.0.1.161 terá um endereço de pesquisa reversa de 161.1.0.10.in-addr.apra, que é um subdomínio de 1.0.10.in-addra.apra.

3. Especifique o servidor para o qual serão encaminhadas essas pesquisas.
4. Adicione essas regras ao endpoint do resolvedor de saída.

Observe que ativar `enableDNSHostNames` para sua VPC adiciona automaticamente registros de PTR. Consulte O que Amazon Route 53 Resolveré. O procedimento anterior é necessário somente se você quiser especificar explicitamente um resolvedor para determinadas faixas IP: por exemplo, ao encaminhar consultas para um servidor do Active Directory.

Associação de regras de encaminhamento a uma VPC

Depois de criar uma regra de encaminhamento, é necessário associá-la a uma ou mais VPCs. As regras só funcionarão depois de serem associadas a uma VPC. Ao associar uma regra a uma VPC, o Resolver começa a encaminhar consultas de DNS do nome de domínio especificado na regra aos resolvedores de DNS especificados na regra. As consultas passam pelo endpoint de saída especificado durante a criação da regra.

Para associar uma regra de encaminhamento a uma ou mais VPCs

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a Região onde a regra foi criada.
4. Escolha o nome da regra que você deseja associar a uma ou mais VPCs.
5. Escolha Associate VPC.
6. Em VPCs that use this rule (VPCs que usam essa regra), selecione as VPCs às quais você deseja associar a regra.
7. Escolha Adicionar.

Desassociação de regras de encaminhamento de uma VPC

Desassocie uma regra de encaminhamento de uma VPC nas seguintes circunstâncias:

- Para consultas de DNS originadas nessa VPC, você quer que o Resolver pare de encaminhar consultas do nome de domínio especificado na regra para sua rede.
- Você deseja excluir a regra de encaminhamento. Se uma regra está atualmente associada a uma ou mais VPCs, é necessário desassociar a regra de todas as VPCs antes de excluí-la.

Se quiser desassociar uma regra de encaminhamento de uma ou mais VPCs, execute o procedimento a seguir.

Para desassociar uma regra de encaminhamento de uma VPC

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a Região onde a regra foi criada.
4. Escolha o nome da regra que deseja desassociar de uma ou mais VPCs.
5. Escolha a opção para a VPC da qual você deseja desassociar a regra.
6. Escolha Desassociar.
7. Digite disassociate para confirmar.
8. Selecione Enviar.

Compartilhamento de regras do Resolvedor com outras AWS contas e uso de regras compartilhadas

Você pode compartilhar as regras do Resolver que você criou usando uma AWS conta com outras AWS contas. Para compartilhar regras, o console do Route 53 Resolver se integra ao AWS Resource Access Manager. Para obter mais informações sobre o Resource Access Manager, consulte o Guia do usuário do Resource Access Manager.

Observe o seguinte:

Associação de regras compartilhadas a VPCs

Se outra AWS conta tiver compartilhado uma ou mais regras com sua conta, você poderá associar as regras às suas VPCs da mesma forma que associa as regras que criou às suas VPCs. Para ter mais informações, consulte Associação de regras de encaminhamento a uma VPC.

Exclusão ou interrupção do compartilhamento de uma regra

Se você compartilhar uma regra com outras contas e, em seguida, excluir a regra ou parar de compartilhá-la, e se a regra foi associada a uma ou mais VPCs, o Route 53 Resolver começará a processar consultas de DNS para essas VPCs com base nas regras restantes. O comportamento é igual ao da desassociação da regra da VPC.

Se uma regra for compartilhada com uma Unidade Organizacional (UO) e uma conta na UO for movida para outra UO, todas as associações com a regra compartilhada com qualquer VPC na conta serão excluídas. No entanto, se a regra do Resolver já tiver sido compartilhada com a OU de destino, a associação VPC permanecerá intacta e não será dissociada.

Número máximo de regras e associações

Quando uma conta cria uma regra e a compartilha com uma ou mais outras contas, o número máximo de regras por AWS região se aplica à conta que criou a regra.

Quando uma conta com a qual uma regra é compartilhada associa a regra a uma ou mais VPCs, o número máximo de associações entre regras e VPCs por região se aplicará à conta com a qual a regra está compartilhada.

Para as cotas atuais do Resolver, consulte Cotas no Route 53 Resolver.

Permissões

Para compartilhar uma regra com outra AWS conta, você precisa ter permissão para usar a PutResolverRulePolicyação.

Restrições na AWS conta com a qual uma regra é compartilhada

A conta com a qual uma regra é compartilhada não pode alterar ou excluir a regra.

Tags

Somente a conta que criou uma regra pode adicionar, excluir ou consultar tags na regra.

Para visualizar o status de compartilhamento atual de uma regra (incluindo a conta que compartilhou a conta ou a conta com a qual uma regra é compartilhada) e para compartilhar regras com outra conta, realize o procedimento a seguir.

Para ver o status de compartilhamento e as regras de compartilhamento com outra AWS conta

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a Região onde a regra foi criada.

   A coluna Sharing status (Status de compartilhamento) mostra o status de compartilhamento atual das regras criadas pela conta atual ou que foram compartilhadas com a conta atual:

   - Não compartilhada: a AWS conta atual criou a regra e a regra não é compartilhada com nenhuma outra conta.
   - Shared by me (Compartilhada por mim): a conta atual criou a regra e compartilhou com uma ou mais contas.
   - Shared with me (Compartilhada comigo): outra conta criou a regra e compartilhou com a conta atual.
4. Escolha o nome da regra para a qual deseja exibir informações de compartilhamento ou que deseja compartilhar com outra conta.

   Na página Rule: ***rule name*** (Regra: nome da regra), o valor em Owner (Proprietário) exibe o ID da conta da que criou a regra. Essa é a conta atual, a menos que o valor do Sharing status (Status de compartilhamento) seja Shared with me (Compartilhada comigo). Neste caso, Owner (Proprietário) é a conta que criou a regra e compartilhou com a conta atual.
5. Escolha Share (Compartilhar) para visualizar informações adicionais ou para compartilhar a regra com outra conta. Uma página no console do Resource Access Manager é exibida, dependendo do valor de Sharing status (Status de compartilhamento):

   - Não compartilhada: a página Create resource share (Criar compartilhamento de recurso) é exibida. Para obter informações sobre como compartilhar a regra com outra conta, OU ou organização, pule para a etapa 6.
   - Compartilhada por mim: a página Shared resources (Recursos compartilhados) mostra as regras e outros recursos de propriedade da conta atual e compartilhados com outras contas.

- Compartilhada comigo: a página Shared resources (Recursos compartilhados) mostra as regras e outros recursos de propriedade de outras contas e compartilhados com a conta atual.

6. Para compartilhar uma regra com outra AWS conta, OU ou organização, especifique os valores a seguir.

> **Note**
>
> Não é possível atualizar as configurações de compartilhamento. Se quiser alterar qualquer uma das configurações a seguir, é necessário compartilhar a regra novamente com as novas configurações e, em seguida, remover as configurações de compartilhamento antigas.

Descrição

Insira uma breve descrição que te ajude a lembrar o motivo do compartilhamento da regra.

Recursos

Marque a caixa de seleção da regra que deseja compartilhar.

Entidades principais

Insira o número da AWS conta, nome da OU ou nome da organização.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Essas são as tags que AWS Billing and Cost Management permitem organizar sua AWS fatura; você também pode usar tags para outros fins. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing .

Excluir regras de encaminhamento

Para excluir uma regra de encaminhamento, execute o procedimento a seguir.

Observe o seguinte:

- Se a regra de encaminhamento estiver associada a alguma VPC, é necessário desassociar a regra dessas VPCs antes de excluí-la. Para ter mais informações, consulte Desassociação de regras de encaminhamento de uma VPC.
- Você não pode excluir a regra padrão Internet Resolver (Resolvedor de Internet), que tem um valor de Recursive (Recursivo) para Type (Tipo). Essa regra faz com que o Resolver do Route 53 atue como um resolvedor recursivo para todos os nomes de domínio para os quais você não criou regras personalizadas e para os quais o Resolver não criou regras definidas automaticamente. Para obter mais informações sobre como as regras são categorizadas, consulte Uso de regras para controlar quais consultas são encaminhadas para sua rede.

Para excluir uma regra de encaminhamento

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Regras.
3. Na barra de navegação, escolha a Região onde a regra foi criada.
4. Escolha a opção da regra que deseja excluir.
5. Escolha Excluir.
6. Para confirmar a exclusão da regra, insira o nome da regra e escolha Submit (Enviar).

Regras de encaminhamento para consultas DNS reversas no Resolver

Quando `enableDnsHostnames` e `enableDnsSupport` estão definidos como `true` para uma nuvem privada virtual (VPC) do Amazon VPC, o Resolver cria regras de sistema definidas automaticamente para consultas de DNS reversas. Para saber mais sobre essas configurações, consulte o tópico sobre Atributos de DNS na sua VPC, no Guia do Desenvolvedor da Amazon VPC.

Regras de encaminhamento para consultas de DNS reverso são especialmente úteis para serviços como SSH ou Active Directory, que têm a opção de autenticar usuários realizando uma pesquisa de DNS reverso para o endereço IP do qual um usuário está tentando se conectar a um recurso. Para obter mais informações sobre regras de sistema automaticamente definidas, consulte Nomes de domínio para os quais o Resolver cria regras de sistema autodefinidas.

É possível desativar essas regras e modificar todas as consultas de DNS reverso para que elas sejam, por exemplo, encaminhadas aos seus servidores de nomes on-premises para resolução.

Após desativar as regras automáticas, crie regras para encaminhar as consultas aos seus recursos on-premises de acordo com a necessidade. Para saber mais sobre como gerenciar regras de encaminhamento, consulte Gerenciamento de regras de encaminhamento.

Para desativar regras automaticamente definidas

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, em Resolver, escolha VPCs e depois um ID de VPC.
3. Em Autodefined rules for reverse DNS resolution (Regras automaticamente definidas para resolução de DNS reverso), desmarque a caixa de seleção. Se a caixa de seleção já estiver desmarcada, você poderá marcá-la para ativar a resolução de DNS reverso automaticamente definida.

Para as APIs relacionadas, consulte APIs de configuração do Resolver.

Como habilitar validação de DNSSEC no Amazon Route 53

Quando você habilita a validação de DNSSEC para uma nuvem privada virtual (VPC) no Amazon Route 53, as assinaturas de DNSSEC são verificadas criptograficamente para garantir que a resposta não tenha sido adulterada. Você habilita a validação de DNSSEC na página de detalhes da VPC.

A validação de DNSSEC é aplicada pelo Route 53 Resolver a nomes públicos assinados quando ele está executando uma resolução de DNS recursiva.

Porém, se o Route 53 Resolver estiver encaminhando para outro resolver de DNS, esse resolver estará executando uma resolução de DNS recursiva e, portanto, também deverá aplicar a validação de DNSSEC.

> **Important**
>
> A ativação da validação de DNSSEC pode afetar a resolução DNS para registros DNS públicos dos recursos da AWS em uma VPC, o que pode resultar em uma interrupção. Observe que habilitar ou desabilitar a validação de DNSSEC pode levar vários minutos.

> **Note**
>
> No momento, o Amazon Route 53 Resolver em sua VPC (também conhecido como AmazonProvided DNS) ignora o bit do cabeçalho DO (DNSSEC OK) EDNS e o bit CD (Checking Disabled) na consulta DNS. Se você configurou DNSSEC, isso significa que, embora o Route 53 Resolver faça a validação DNSSEC, ele não retorna registros DNSSEC nem define o bit AD na resposta. Portanto, fazer sua própria validação DNSSEC não é compatível com o Resolvedor Route 53 no momento. Se você precisar fazer isso, terá que fazer sua própria resolução recursiva de DNS.

Para habilitar a validação DNSSEC para uma VPC

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, em Resolver, escolha VPCs.
3. Em Validação de DNSSEC, marque a caixa de seleção. Se a caixa de seleção já estiver marcada, você poderá desmarcá-la para desabilitar a validação de DNSSEC.

   Observe que habilitar ou desabilitar a validação de DNSSEC pode levar vários minutos.

Encaminhando o tráfego da Internet para seus recursos AWS

Você pode usar o Amazon Route 53 para direcionar o tráfego para uma variedade de AWS recursos.

- Encaminhar o tráfego para uma API do Amazon API Gateway por meio do seu nome de domínio
- Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio
- Como encaminhar o tráfego para uma instância do Amazon EC2
- Roteamento do tráfego para um serviço AWS App Runner
- Roteamento do tráfego para um ambiente AWS Elastic Beanstalk
- Rotear tráfego para um load balancer do ELB
- Como encaminhar o tráfego para um site hospedado em um bucket do Amazon S3
- Como encaminhar o tráfego para um endpoint de interface da Amazon Virtual Private Cloud por meio do seu nome de domínio
- Roteamento de tráfego para a Amazon WorkMail
- Roteamento de tráfego para outros recursos AWS
- Como criar recursos do Amazon Route 53 e do Amazon Route 53 Resolver com o AWS CloudFormation

Encaminhar o tráfego para uma API do Amazon API Gateway por meio do seu nome de domínio

É possível usar o Amazon API Gateway para criar, publicar, manter, monitorar e proteger APIs. Você pode criar APIs que acessam AWS serviços ou outros serviços da web, além dos dados armazenados na AWS nuvem.

O método usado para encaminhar o tráfego de domínio para uma API do API Gateway é o mesmo, independentemente de você ter criado um endpoint regional do API Gateway ou um endpoint do API Gateway otimizado para bordas.

- Endpoint de API regional: crie um registro de alias do Route 53 que encaminha o tráfego para o endpoint de API regional.

- Endpoint da API otimizado para borda: é criado um registro de alias do Route 53 que encaminha o tráfego para a API otimizada para borda. Isso faz com que o tráfego seja roteado para a CloudFront distribuição associada à API otimizada para borda.

Um registro de alias é uma extensão do Route 53 para DNS semelhante a um registro CNAME. Para obter uma comparação de registros de alias e CNAME, consulte Escolher entre registros de alias e não alias.

> **Note**
>
> O Route 53 não cobra por consultas de alias às APIs do API Gateway ou outros recursos. AWS

Tópicos

Pré-requisitos

Para começar, faça o seguinte:

- Uma API do API Gateway que tem um nome de domínio personalizado, como api.example.com que corresponda ao nome do registro do Route 53 que você deseja criar.

  Para obter mais informações, consulte os tópicos a seguir.

  - Configurar nomes de domínio personalizados para APIs HTTP no Guia do desenvolvedor do Amazon API Gateway.
  - Configurar nomes de domínio personalizados para APIs REST no Guia do desenvolvedor do Amazon API Gateway.
  - Configuração de nomes de domínio personalizados para WebSocket APIs no Guia do desenvolvedor do Amazon API Gateway.
- Um nome de domínio registrado. Você pode usar o Amazon Route 53 como seu registrador de domínio ou pode usar um registrador diferente.

- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Como configurar o Route 53 para encaminhar o tráfego para um endpoint do API Gateway

Para configurar o Route 53 para encaminhar o tráfego para um endpoint do API Gateway, siga o procedimento a seguir.

Para encaminhar o tráfego para um endpoint do API Gateway

1. Se você criou a zona hospedada do Route 53 e o endpoint regional usando a mesma conta, vá para a etapa 2.

   Se você criou a zona hospedada e o endpoint regional usando contas diferentes, obtenha o nome de domínio de destino para o nome de domínio personalizado que você deseja usar:

   a. Faça login AWS Management Console e abra o console do API Gateway em https://console.aws.amazon.com/apigateway/.
   b. No painel de navegação, selecione Nomes de domínio personalizados.
   c. Selecione o nome de domínio personalizado que você deseja usar e obtenha o valor de API Gateway domain name (Nome de domínio do API Gateway).
2. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Selecione o nome da zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para sua API.
5. Escolha Create record (Criar registro).
6. Especifique os seguintes valores:

Política de roteamento

Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

Nome de registro

Insira o nome de domínio que você deseja usar para rotear o tráfego para sua API.

A API para a qual você deseja encaminhar o tráfego deve incluir um nome de domínio personalizado, como api.example.com que corresponda ao nome do registro do Route 53.

Alias

Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

Valor/Encaminhar tráfego para

Escolha Alias to API Gateway API (Alias para API do API Gateway) e, em seguida, escolha a região de origem do endpoint.

A forma como você especifica o valor do Endpoint depende se você criou a zona hospedada e a API usando a mesma AWS conta ou contas diferentes:

- Same account (Mesma conta): a lista de nomes de domínio de destino inclui apenas as APIs que têm um nome de domínio personalizado que corresponde ao valor que você especificou em Record name (Nome do registro). Selecione o valor aplicável.
- Different accounts (Diferentes contas): insira o valor que você obteve na etapa 1 deste procedimento.

Tipo de registro

Escolha A - IPv4 address (A – Endereço IPv4).

Avaliar status do alvo

Para controlar o failover de DNS, configure verificações de integridade personalizadas. Para ver um exemplo, consulte Configurar verificações de integridade personalizadas para failover de DNS no Guia do usuário do API Gateway.

7. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá rotear o tráfego para sua API usando o nome do registro de alias que você criou neste procedimento.

Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio

Você pode usar a Amazon CloudFront, a rede de distribuição de AWS conteúdo (CDN), como uma forma de acelerar a entrega do seu conteúdo da web. CloudFront pode fornecer todo o seu site, incluindo conteúdo dinâmico, estático, de streaming e interativo, usando uma rede global de pontos de presença. Os usuários que solicitarem conteúdo serão roteados automaticamente para local da borda que oferecer a menor latência.

> **Note**
>
> Você pode rotear o tráfego para uma CloudFront distribuição somente para zonas hospedadas públicas.

Para usar CloudFront para distribuir o conteúdo do seu site, crie uma distribuição e especifique as configurações para ela. Por exemplo, especifique o bucket Amazon S3 ou o servidor HTTP do qual você CloudFront deseja obter seu conteúdo, se deseja que somente usuários selecionados tenham acesso ao seu conteúdo e se deseja que os usuários usem HTTPS.

Quando você cria uma distribuição, CloudFront atribui um nome de domínio à distribuição, comod111111abcdef8.cloudfront.net. Você pode usar esse nome de domínio nos URLs do seu conteúdo, por exemplo:

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

Se preferir, pode usar seu próprio nome de domínio nos URLs, por exemplo:

```
http://example.com/logo.jpg
```

Siga as etapas do Amazon CloudFront Developer Guide para usar seu próprio nome de domínio nos URLs dos seus arquivos em uma CloudFront distribuição, em vez do nome de domínio atribuído à sua CloudFront distribuição. Para obter mais informações sobre como usar seu próprio nome

de domínio com uma CloudFront distribuição, consulte Usando URLs personalizados adicionando nomes de domínio alternativos (CNAMEs).

Ao usar um nome de domínio do Route 53 com uma CloudFront distribuição, use o Amazon Route 53 para criar um registro de alias que aponta para sua CloudFront distribuição. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como example.com, quanto para subdomínios, como www.example.com. (Você pode criar registros CNAME somente para subdomínios.) Quando o Route 53 recebe uma consulta de DNS que corresponde ao nome e ao tipo de um registro de alias, o Route 53 responde com o nome do domínio associado à sua distribuição.

> **Note**
>
> O Route 53 não cobra por consultas de alias para CloudFront distribuições ou outros recursos. AWS

Pré-requisitos

Para começar, faça o seguinte:

1. Um nome de domínio registrado. Você pode usar o Amazon Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
2. O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

   Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.
3. Solicite um certificado público para que CloudFront as distribuições da Amazon exijam HTTPS. Para obter mais informações, consulte Etapa 2: Solicitar um certificado público e Validação de DNS no AWS Certificate Manager no Guia do usuário AWS Certificate Manager .
4. Uma CloudFront distribuição. A distribuição deve incluir um nome de domínio alternativo que corresponda ao nome de domínio que você deseja usar para seus URLs em vez do nome de domínio CloudFront atribuído à sua distribuição.

Por exemplo, se você deseja que os URLs do seu conteúdo contenham o nome do domínio example.com, o campo Nome de domínio alternativo para a distribuição deve incluir example.com.

Para obter mais informações, consulte a seguinte documentação no Amazon CloudFront Developer Guide:

- Lista de tarefas para criar uma distribuição na Web
- Criando ou atualizando uma distribuição usando o CloudFront console

Configurando o Amazon Route 53 para rotear o tráfego para uma distribuição CloudFront

Para configurar o Amazon Route 53 para rotear o tráfego para uma CloudFront distribuição, siga estas etapas. Para obter mais informações sobre como usar seu próprio nome de domínio com uma CloudFront distribuição, consulte Usando URLs personalizados adicionando nomes de domínio alternativos (CNAMEs) no Amazon CloudFront Developer Guide.

> **Note**
>
> As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando as alterações se propagarem, você poderá rotear o tráfego para sua CloudFront distribuição usando o nome do registro de alias criado neste procedimento.

Para rotear o tráfego para uma distribuição do CloudFront

1. Obtenha o nome de domínio CloudFront atribuído à sua distribuição e determine se o IPv6 está habilitado:

   a. Faça login no AWS Management Console e abra o CloudFront console emhttps://console.aws.amazon.com/cloudfront/v4/home.
   b. na coluna ID selecione o nome vinculado da distribuição para a qual você deseja encaminhar o tráfego (não a caixa de seleção).
   c. Na guia General (Geral), obtenha o valor do campo Distribution domain name (Nome de domínio da distribuição).
   d. Na guia General (Geral), na seção Settings (Configurações), escolha editar e role para verificar o campo IPv6 para ver se o IPv6 está habilitado para a distribuição. Se o IPv6

estiver habilitado, você precisará criar dois registros de alias para a distribuição, um para encaminhar o tráfego do IPv4 para a distribuição e um para encaminhar o tráfego do IPv6. Escolha Cancelar.

Para obter mais informações, consulte Habilitar IPv6 no tópico Valores que você especifica ao criar ou atualizar uma distribuição no Amazon CloudFront Developer Guide.

2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Escolha o nome vinculado da zona hospedada para o domínio que você deseja usar para rotear o tráfego para sua CloudFront distribuição.
5. Escolha Create record (Criar registro).

   Use o assistente para criar os registros ou escolha Switch to quick create (Alternar para criação rápida).
6. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome de domínio que você deseja usar para rotear o tráfego para sua CloudFront distribuição. O valor padrão é o nome da hosted zone.

   Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.example.com (acme.exemplo.com) para rotear o tráfego para sua distribuição, digite acme.

   Alias

   Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

   > **Important**
   >
   > Você deve criar um registro Alias para que a CloudFront distribuição funcione.

Valor/Encaminhar tráfego para

Escolha Apelido para CloudFront distribuições. A região (us-east-1) é selecionada por padrão. Escolha o nome de domínio CloudFront atribuído à distribuição quando você a criou. Esse é o valor que você obteve na etapa 1.

Tipo de registro

Escolha A - IPv4 address (A – Endereço IPv4).

Se o IPv6 estiver habilitado para a distribuição, e você estiver criando um segundo registro, escolha AAAA – IPv6 address (AAAA: endereço IPv6).

Avaliar status do alvo

Aceite o valor padrão de No (Não).

7. Escolha Create records (Criar registros).
8. Se o IPv6 estiver habilitado para a distribuição, repita as etapas de 5 a 7. Especifique as mesmas configurações exceto o campo Tipo de registro, conforme explicado na etapa 6.

Como encaminhar o tráfego para uma instância do Amazon EC2

O Amazon EC2 fornece capacidade de computação escalável na nuvem. AWS Você pode iniciar um ambiente de computação virtual EC2 (uma instância) usando um modelo pré-configurado (uma Imagem de máquina da Amazon ou AMI). Quando você inicia uma instância do EC2, o EC2 instala automaticamente o sistema operacional (Linux ou Microsoft Windows) e o software adicional incluído no AMI, tal como o servidor web ou o software de banco de dados.

Você poderá encaminhar o tráfego do seu domínio, como example.com, ao seu servidor usando o Amazon Route 53, se estiver hospedando um site ou executando uma aplicação Web em uma instância do EC2.

Pré-requisitos

Para começar, faça o seguinte:

- Uma instância do Amazon EC2. Para obter informações sobre como iniciar uma instância do EC2, consulte as documentações a seguir:

- Linux — Consulte Introdução às instâncias Linux do Amazon EC2 no Guia do usuário do Amazon EC2
- Microsoft Windows — Consulte Introdução às instâncias Windows do Amazon EC2 no Guia do usuário do Amazon EC2

> **Important**
>
> Recomendamos que você também crie um Endereço IP elástico e o associe à sua instância do EC2. Um endereço IP elástico garante que o endereço IP da sua instância do Amazon EC2 nunca mudará. Para obter mais informações, consulte Preço para endereços de IP elásticos.

- Um nome de domínio registrado. Você pode usar o Amazon Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Como configurar o Amazon Route 53 para encaminhar o tráfego para uma instância do Amazon EC2

Para configurar o Amazon Route 53 para encaminhar o tráfego para uma instância do EC2, realize o procedimento a seguir.

Para encaminhar o tráfego para uma instância do Amazon EC2

1. Obtenha o endereço IP da instância do Amazon EC2:
   a. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
   b. Na lista de regiões no canto superior direito do console, escolha a região na qual você executou a instância.
   c. No painel de navegação, escolha Instâncias.

d. Na tabela, escolha a instância para a qual você deseja rotear o tráfego.

e. No painel inferior, na guia Descrição, copie o valor de IPs elásticos.

   Se você não associou um IP elástico à instância, copie o valor de IP público IPv4.

2. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Escolha o nome da zona hospedada que corresponde ao nome do domínio para o qual você quer rotear o tráfego.
5. Escolha Create record (Criar registro).
6. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome do domínio que você deseja usar para rotear o tráfego para a sua instância do EC2. O valor padrão é o nome da hosted zone.

   Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para sua instância do EC2, insira acme.

   Valor/Encaminhar tráfego para

   Escolha o endereço IP ou outro valor dependendo do tipo de registro. Insira o endereço IP que você obteve na etapa 1.

   Tipo de registro

   Escolha A - IPv4 address (A – Endereço IPv4).

   TTL (segundos)

   Aceite o valor padrão de 300.

7. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá encaminhar o tráfego para a sua instância do EC2 usando o nome do registro criado neste procedimento.

> **Important**
>
> Se você liberar o IP elástico, lembre-se de excluir também o registro DNS que aponta para ele. Caso contrário, você terá um registro DNS pendurado que pode ser assumido por um usuário não autorizado.

Roteamento do tráfego para um serviço AWS App Runner

AWS App Runner é um serviço totalmente gerenciado que facilita aos desenvolvedores a implantação de aplicativos web e APIs em contêineres em grande escala e sem a necessidade de experiência prévia em infraestrutura. Comece com seu código-fonte ou uma imagem de contêiner. O App Runner cria e implanta o aplicativo web automaticamente, equilibra a carga do tráfego com criptografia, escala para atender às suas necessidades de tráfego e facilita a comunicação de seus serviços com outros AWS serviços e aplicativos executados em uma Amazon VPC privada. Com o App Runner, em vez de pensar em servidores ou escalabilidade, você tem mais tempo para se concentrar em seus aplicativos. Para obter mais informações, consulte O que é o AWS App Runner? no Guia do desenvolvedor do AWS App Runner .

> **Important**
>
> Atualmente, o Amazon Route 53 oferece suporte a registros de alias para AWS App Runner serviços criados após 1º de agosto de 2022.

Para encaminhar o tráfego do domínio para um serviço do App Runner, use o Amazon Route 53 e crie um registro de alias que aponte para seu serviço do App Runner. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como example.com, quanto para subdomínios, como www.example.com (http://www.example.com/). Você pode criar somente registros CNAME para subdomínios.

> **Note**
>
> Não há cobranças do Route 53 por consultas de alias para serviço do App Runner nem para outros recursos da AWS .

Pré-requisitos

Para começar, faça o seguinte:

- Um serviço do App Runner. Para obter informações sobre como criar um serviço do App Runner, consulte Introdução ao App Runner.
- Um nome de domínio registrado. Você pode usar o Amazon Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.
- Associar o domínio personalizado ao serviço do App Runner. Para obter mais informações, consulte Gerenciamento de nomes de domínio personalizados para um serviço do App Runner.
- Configure o registro de validação do certificado retornado pelo App Runner para sua zona hospedada do Route 53 para iniciar o processo de validação do domínio. Para obter mais informações, consulte validação de DNS no AWS Certificate Manager no Guia do usuário AWS Certificate Manager .

Configurar o Amazon Route 53 para direcionar o tráfego para um serviço do App Runner

Para configurar o Amazon Route 53 para encaminhar o tráfego para um serviço do App Runner, realize o procedimento a seguir.

Para direcionar o tráfego para um serviço do App Runner

1. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha o nome da zona hospedada que corresponde ao nome do domínio para o qual você quer rotear o tráfego.
4. Escolha Create record (Criar registro).
5. Especifique os seguintes valores:

Política de roteamento

Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

Nome de registro

Insira o nome de domínio que você deseja usar para rotear o tráfego para seu serviço do App Runner. O valor padrão é o nome da hosted zone.

Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para seu serviço do App Runner, digite acme.

Valor/Encaminhar tráfego para

Escolha Alias para o serviço do App Runner e, em seguida, escolha o Região da AWS. Escolha o nome de domínio do ambiente para o qual você deseja encaminhar o tráfego.

Tipo de registro

Aceite o valor padrão, A – endereço IPv4.

Avaliar status do alvo

Aceite o valor padrão de Yes (Sim).

6. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá rotear o tráfego para seu serviço do App Runner usando o nome do registro de alias que você criou neste procedimento.

Roteamento do tráfego para um ambiente AWS Elastic Beanstalk

Se você estiver usando AWS Elastic Beanstalk para implantar e gerenciar aplicativos na AWS nuvem, você pode usar o Amazon Route 53 para rotear o tráfego de DNS do seu domínio, como example.com, para um ambiente novo ou existente do Elastic Beanstalk.

Para encaminhar o tráfego de DNS para um ambiente do Elastic Beanstalk, veja os procedimentos nos tópicos a seguir.

> **Note**
>
> Estes procedimentos presumem que você já esteja usando o Route 53 como serviço DNS para o seu domínio. Se você estiver usando outro serviço DNS, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio.

Tópicos

Como implantar aplicações em um ambiente do Elastic Beanstalk

Se você já tiver um ambiente do Elastic Beanstalk para o qual queira encaminhar o tráfego, vá para Como obter o nome de domínio do ambiente do Elastic Beanstalk.

Para criar uma aplicação e implantá-la em um ambiente do Elastic Beanstalk

- Para obter informações sobre como criar uma aplicação e implantá-la em um ambiente do Elastic Beanstalk, consulte Conceitos básicos do Elastic Beanstalk no Guia do desenvolvedor do AWS Elastic Beanstalk .

Como obter o nome de domínio do ambiente do Elastic Beanstalk

Se você já sabe o nome de domínio do seu ambiente do Elastic Beanstalk, vá para Como criar um registro do Amazon Route 53 que encaminha o tráfego para o seu ambiente do Elastic Beanstalk.

Para obter o nome de domínio do ambiente do Elastic Beanstalk

1. Faça login AWS Management Console e abra o console do Elastic Beanstalk em https://console.aws.amazon.com/elasticbeanstalk/.
2. Na lista de aplicativos, encontre o aplicativo para o qual você deseja rotear o tráfego e obtenha o valor de URL. No painel de navegação, escolha Applications (Aplicações) e selecione a aplicação na lista.

Para obter mais informações sobre o URL, consulte Nome de domínio do ambiente do Elastic Beanstalk, no Guia do Desenvolvedor do Elastic Beanstalk.

Como criar um registro do Amazon Route 53 que encaminha o tráfego para o seu ambiente do Elastic Beanstalk

Um registro do Amazon Route 53 contém as configurações que controlam como o tráfego é encaminhado para seu ambiente do Elastic Beanstalk. Crie um registro CNAME ou um registro de alias, dependendo se o nome de domínio para o ambiente inclui a região, como us-east-2, em que você implantou o ambiente. Novos ambientes incluem a região no nome de domínio, mas não ambientes criados antes do início de 2016. Para uma comparação dos registros CNAME e de alias, consulte Escolher entre registros de alias e não alias.

Se o nome de domínio não incluir a região

Você precisará criar um registro CNAME. No entanto, devido a limitações impostas pelo DNS, você pode criar registros CNAME somente para subdomínios, e não para o nome de domínio raiz. Por exemplo, se o nome de seu domínio for exemplo.com, você poderá criar um registro que direciona o tráfego de acme.exemplo.com para seu ambiente do Elastic Beanstalk, mas não poderá criar um registro que direcione o tráfego de exemplo.com para seu ambiente do Elastic Beanstalk.

Consulte o procedimento Para criar um registro CNAME para encaminhar o tráfego para um ambiente do Elastic Beanstalk.

Se o nome de domínio incluir a região

Você pode criar um registro de alias. Um registro de alias é específico para o Route 53 e tem duas vantagens significativas em relação aos registros CNAME:

- Você pode criar registros de alias para o nome de domínio raiz ou para subdomínios. Por exemplo, se o seu nome de domínio for example.com, você poderá criar um registro que encaminha solicitações de example.com ou acme.example.com para o seu ambiente do Elastic Beanstalk.
- Não há cobrança do Route 53 por solicitações que usam um registro de alias para encaminhar o tráfego.

Consulte o procedimento Para criar um registro de alias do Amazon Route 53 para encaminhar o tráfego para um ambiente do Elastic Beanstalk.

Para criar um registro CNAME para encaminhar o tráfego para um ambiente do Elastic Beanstalk

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha o nome da zona hospedada que você quer usar para encaminhar o tráfego para o seu ambiente do Elastic Beanstalk.
4. Escolha Create record (Criar registro).
5. Escolha Alternar para criar rapidamente
6. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome do domínio que você deseja usar para rotear o tráfego para o seu ambiente do Elastic Beanstalk. O valor padrão é o nome da hosted zone.

   Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para seu ambiente, insira acme.

   > **Important**
   >
   > Não é possível criar um registro CNAME que tenha o mesmo nome que a zona hospedada.

   Alias

   Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

   Valor/Encaminhar tráfego para

   Escolha o endereço IP ou outro valor dependendo do tipo de registro e insira o valor que você obtém quando executa o procedimento no tópico Como obter o nome de domínio do ambiente do Elastic Beanstalk. Se tiver usado contas diferentes para criar a zona hospedada

do Route 53 e o ambiente do Elastic Beanstalk, insira os atributos CNAME para o ambiente do Elastic Beanstalk.

Tipo de registro

Escolha CNAME.

TTL (segundos)

Aceite o valor padrão de 300.

7. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos.

Para criar um registro de alias do Amazon Route 53 para encaminhar o tráfego para um ambiente do Elastic Beanstalk

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha o nome da zona hospedada que você quer usar para encaminhar o tráfego para o seu ambiente do Elastic Beanstalk.
4. Escolha Create record (Criar registro).
5. Especifique os seguintes valores:

Política de roteamento

Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

Nome de registro

Insira o nome do domínio que você deseja usar para rotear o tráfego para o seu ambiente do Elastic Beanstalk. O valor padrão é o nome da hosted zone.

Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para seu ambiente, insira acme.

Valor/Encaminhar tráfego para

Escolha Alias to Elastic Beanstalk environment (Alias para o ambiente do Elastic Beanstalk) e, em seguida, escolha a região de origem do endpoint. Escolha o nome de domínio do ambiente para o qual você deseja encaminhar o tráfego. Este é o valor que você obtém quando executa o procedimento no tópico Como obter o nome de domínio do ambiente do Elastic Beanstalk.

Se tiver usado contas diferentes para criar a zona hospedada do Route 53 e o ambiente do Elastic Beanstalk, insira o atributo CNAME para o ambiente do Elastic Beanstalk.

Tipo de registro

Aceite o padrão, A – IPv4 address (A: endereço IPv4).

Avaliar status do alvo

Aceite o valor padrão de Yes (Sim).

6. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá encaminhar o tráfego para o seu ambiente do Elastic Beanstalk usando o nome do registro de alias criado neste procedimento.

Rotear tráfego para um load balancer do ELB

Se hospedar um site em várias instâncias do Amazon EC2, você poderá distribuir o tráfego para seu site através das instâncias usando um balanceador de carga do Elastic Load Balancing (ELB). O serviço do ELB escala automaticamente o load balancer conforme o tráfego para o seu site sofre mudanças. O load balancer também pode monitorar a integridade das suas instâncias registradas e rotear somente o tráfego de domínio para instâncias íntegras.

Para encaminhar o tráfego do domínio para um balanceador de carga do ELB, use o Amazon Route 53 e crie um registro de alias que aponte para seu balanceador de carga. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como example.com, quanto para subdomínios, como www.example.com. (Você pode criar registros CNAME somente para subdomínios.)

> **Note**
>
> Não há cobranças do Route 53 por consultas de alias para balanceadores de carga do ELB nem para outros recursos da AWS .

Pré-requisitos

Para começar, faça o seguinte:

- Um balanceador de carga do ELB. Você pode usar o Classic Load Balancer, Application Load Balancer ou o Network Load Balancer ELB. Para obter informações sobre a criação de um balanceador de carga, consulte Conceitos básicos do Elastic Load Balancing no Manual do usuário do Elastic Load Balancing.

  Nomeie o load balancer para lembrar mais tarde qual a finalidade dele. O nome que você especificar ao criar um balanceador de carga é o nome que você escolherá ao criar um registro de alias no console do Route 53.
- Um nome de domínio registrado. Você pode usar o Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Configurar o Amazon Route 53 para encaminhar o tráfego para um balanceador de carga do ELB

Para configurar o Amazon Route 53 para encaminhar o tráfego para um balanceador de carga do ELB, realize o procedimento a seguir.

Para rotear o tráfego para um load balancer do ELB

1. Se você criou a zona hospedada do Route 53 e o balanceador de carga do ELB usando a mesma conta, vá para a etapa 2.

   Se você criou a zona hospedada e o load balancer do ELB usando contas diferentes, execute o procedimento Obter o nome do DNS para um balanceador de carga de Elastic Load Balancing para obter o nome do DNS do load balancer.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, escolha Zonas hospedadas.
4. Escolha o nome da zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para o seu load balancer.
5. Escolha Create record (Criar registro).
6. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome do domínio ou do subdomínio que você deseja usar para rotear o tráfego para o seu load balancer do ELB. O valor padrão é o nome da hosted zone.

   Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para o seu load balancer, insira acme.

   Alias

   Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

   Valor/Encaminhar tráfego para

   Escolha Alias to Application and Classic Load Balancer (Alias para aplicação e balanceador de carga clássico) ou Alias to Network Load Balancer (Alias para Network Load Balancer) e, em seguida, escolha a região de origem do endpoint.

Se você criou a zona hospedada e o balanceador de carga ELB usando a mesma AWS conta, escolha o nome que você atribuiu ao balanceador de carga ao criá-lo.

Se você tiver criado a zona hospedada e o load balancer do ELB usando contas diferentes, insira o valor que você obteve na etapa 1 deste procedimento.

> **Note**
>
> O console precede o dualstack. para o nome DNS do aplicativo e Classic Load Balancer somente da AWS mesma conta. Quando um cliente, como um navegador da Web, solicita o endereço IP para o seu nome de domínio (example.com) ou nome do subdomínio (www.example.com), o cliente pode solicitar um endereço IPv4 (um registro A), um endereço IPv6 (um registro AAAA), ou ambos (em solicitações separadas). A designação dualstack. permite que o Route 53 responda com o endereço IP apropriado ao seu balanceador de carga com base no formato de endereço IP que o cliente solicitou. Você precisará preceder dualstack. para o Application Load Balancer e o Classic Load Balancer da conta diferente.

Tipo de registro

Escolha A - IPv4 address (A – Endereço IPv4).

Avaliar status do alvo

Se quiser encaminhar o tráfego do Route 53 com base na integridade dos seus recursos, escolha Yes (Sim). Para obter mais informações sobre como verificar a integridade dos seus recursos, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

7. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá encaminhar o tráfego para o seu load balancer; usando o nome do registro de alias criado neste procedimento.

Como encaminhar o tráfego para um site hospedado em um bucket do Amazon S3

O Amazon Simple Storage Service (Amazon S3) oferece um armazenamento na nuvem altamente escalável, seguro e duradouro. Você pode configurar um bucket do S3 para hospedar um site estático que pode incluir páginas da web e scripts do lado do cliente. (O S3 não oferece suporte para script de servidor.)

Para encaminhar o tráfego do domínio para um bucket do S3, use o Amazon Route 53 e crie um registro de alias que aponte para seu bucket. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como example.com, quanto para subdomínios, como www.example.com. Você pode criar registros CNAME somente para subdomínios.

> **Note**
>
> O Route 53 não cobra por consultas de alias em buckets do S3 ou outros recursos. AWS

Pré-requisitos

Para começar, faça o seguinte. Se você não estiver familiarizado com o Amazon Route 53 ou o S3, consulte Conceitos básicos do Amazon Route 53, que fornece orientações durante todo o processo, incluindo como registrar um nome de domínio e como criar e configurar um bucket do S3.

- Um bucket do S3 configurado para hospedar um site estático.

  Para obter mais informações, consulte o tópico sobre como Configurar um bucket para hospedagem do sites, no Guia do usuário do Amazon Simple Storage Service.

  > **Important**
  >
  > O bucket precisa ter o mesmo nome que o seu domínio ou subdomínio. Por exemplo, se você quiser usar o nome de subdomínio acme.example.com, o nome do bucket deverá ser acme.example.com.

Você pode rotear o tráfego para um domínio e os subdomínios dele, como example.com e www.example.com, para um único bucket. Crie um bucket para o domínio e cada subdomínio e configure todos buckets, exceto um para redirecionar o tráfego para o bucket restante. Para ter mais informações, consulte Conceitos básicos do Amazon Route 53.

> **Note**
>
> Um bucket do S3 configurado como um endpoint do site não é compatível com SSL/TLS, então você precisa rotear o tráfego para a CloudFront distribuição e usar o bucket do S3 como origem da distribuição.
>
> Para obter instruções sobre como criar uma CloudFront distribuição, consulte Criar uma CloudFront distribuição e Configurar nomes de domínio alternativos e HTTPS no Guia do CloudFront Usuário, além deRoteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio.

- Um nome de domínio registrado. Você pode usar o Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Configurar o Amazon Route 53 para encaminhar o tráfego para um bucket do S3

Para configurar o Amazon Route 53 para encaminhar o tráfego para um bucket do S3 configurado para hospedar um site estático, execute o procedimento a seguir.

Para rotear o tráfego para um bucket do S3

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

3. Escolha o nome da zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para o seu bucket do S3.
4. Escolha Create record (Criar registro).
5. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome do domínio que você deseja usar para rotear o tráfego para o seu bucket do S3. O valor padrão é o nome da hosted zone.

   Por exemplo, se o nome da zona hospedada for exemplo.com e você quiser usar acme.exemplo.com para rotear o tráfego para seu bucket, digite acme.

   Alias

   Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

   Valor/Encaminhar tráfego para

   Escolha Alias para endpoint do site do S3 e, em seguida, escolha a região de origem do endpoint.

   Escolha o bucket com o mesmo nome que você especificou para Record name (Nome de registro).

   A lista inclui um bucket somente se o bucket atender aos seguintes requisitos:

   - O nome do bucket é o mesmo que o nome do registro que você está criando.
   - O bucket está configurado como um endpoint de site.
   - O bucket foi criado pela AWS conta corrente.

     Se você criou o bucket usando uma AWS conta diferente, insira o nome da região na qual você criou seu bucket do S3. Para obter o formato correto para o nome da região, consulte a coluna Website endpoint na tabela Amazon S3 website endpoints no Referência geral da Amazon Web Services.

Tipo de registro

Escolha A - IPv4 address (A – Endereço IPv4).

Avaliar status do alvo

Aceite o valor padrão de Yes (Sim).

6. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá encaminhar o tráfego para o seu bucket do S3 usando o nome do registro de alias criado neste procedimento.

Como encaminhar o tráfego para um endpoint de interface da Amazon Virtual Private Cloud por meio do seu nome de domínio

Você pode usar AWS PrivateLink para acessar serviços selecionados com um endpoint de interface da Amazon Virtual Private Cloud (Amazon VPC). Esses serviços incluem alguns AWS serviços, serviços hospedados por outros AWS clientes e parceiros em suas próprias VPCs e serviços de AWS Marketplace parceiros compatíveis.

Para encaminhar o tráfego de domínio para um endpoint de interface, use o Amazon Route 53 para criar um registro de alias. Um registro de alias é uma extensão do Route 53 para DNS. Ele é semelhante a um registro CNAME, mas você pode criar um registro de alias tanto para o domínio raiz, como example.com, quanto para subdomínios, como www.example.com. Você pode criar registros CNAME somente para subdomínios.

> **Note**
>
> O Route 53 não cobra por consultas de alias em endpoints de interface ou outros recursos. AWS

Tópicos

Pré-requisitos

Para começar, faça o seguinte:

- Um endpoint de interface da Amazon VPC. Para obter mais informações, consulte Interface VPC endpoints (AWS PrivateLink) no Guia do usuário da Amazon VPC.
- Um nome de domínio registrado. Você pode usar o Amazon Route 53 como seu registrador de domínio ou pode usar um registrador diferente.
- O Route 53 como serviço de DNS para o domínio. Se você registrar seu nome de domínio usando o Route 53, nós configuraremos automaticamente o Route 53 como o serviço de DNS para o domínio.

  Para obter informações sobre como usar o Route 53 como o provedor de serviços DNS de seu domínio, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.

Como configurar o Amazon Route 53 para encaminhar o tráfego para um endpoint de interface da Amazon VPC

Para configurar o Amazon Route 53 para encaminhar o tráfego para um endpoint de interface da Amazon VPC, siga o procedimento a seguir.

Para rotear o tráfego para um endpoint de interface da Amazon VPC

1. Se você criou a zona hospedada do Route 53 e o endpoint de interface da Amazon VPC usando a mesma conta, vá para a etapa 2.

   Se você criou a zona hospedada e o endpoint de interface usando contas diferentes, obtenha o nome do serviço para o endpoint de interface:

   a. Faça login AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
   b. No painel de navegação, escolha Endpoints.
   c. No painel direito, selecione o endpoint para o qual você deseja rotear o tráfego de Internet.
   d. No painel inferior, obtenha o valor de nome do DNS, por exemplo, vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com.
2. Abra o console do Route 53 em https://console.aws.amazon.com/route53/.

3. No painel de navegação, escolha Zonas hospedadas.
4. Escolha o nome da zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para seu endpoint de interface.
5. Escolha Create record (Criar registro).
6. Especifique os seguintes valores:

   Política de roteamento

   Selecione a política de roteamento aplicável. Para ter mais informações, consulte Escolher uma política de roteamento.

   Nome de registro

   Insira o nome de domínio que você deseja usar para encaminhar o tráfego para seu endpoint de interface da Amazon VPC.

   Alias

   Se você estiver usando o método de criação de registro Quick create (Criação rápida), ative o Alias.

   Valor/Encaminhar tráfego para

   Escolha Alias to VPC endpoint (Alias para endpoint da VPC) e, em seguida, escolha a região de origem do endpoint.

   A forma como você especifica o valor dos Endpoints depende se você criou a zona hospedada e o endpoint da interface usando a mesma AWS conta ou contas diferentes:

   - Same account (Mesma conta): escolha a lista e encontre a categoria Amazon VPC endpoints (Endpoints da Amazon VPC). Em seguida, selecione o nome do DNS do endpoint de interface para a qual você deseja rotear o tráfego de Internet.
   - Different accounts (Diferentes contas): insira o valor que você obteve na etapa 1 deste procedimento.

   Tipo de registro

   Escolha A - IPv4 address (A – Endereço IPv4).

   Avaliar status do alvo

   Aceite o valor padrão de Yes (Sim).

7. Escolha Create records (Criar registros).

As alterações geralmente são propagadas para todos os servidores do Route 53 dentro de 60 segundos. Quando a propagação for concluída, você poderá rotear o tráfego para seu endpoint de interface usando o nome do registro de alias que você criou neste procedimento.

Roteamento de tráfego para a Amazon WorkMail

Você pode usar o Route 53 para direcionar o tráfego para seu domínio de WorkMail e-mail da Amazon. O nome da sua zona hospedada do Route 53 (como exemplo.com) deve corresponder ao nome de um domínio da Amazon WorkMail .

> **Note**
>
> Você pode rotear o tráfego para um WorkMail domínio da Amazon somente para zonas públicas hospedadas.

Para rotear o tráfego para a Amazon WorkMail, execute os quatro procedimentos a seguir.

Para configurar o Amazon Route 53 como seu serviço de DNS e adicionar uma WorkMail organização e um domínio de e-mail da Amazon

1. Se você não registrou o nome de domínio que deseja usar nos seus endereços de e-mail (como john@example.com), registre o domínio agora e verifique se ele está disponível. Para ter mais informações, consulte Registrar um novo domínio.

   Se o Amazon Route 53 não for o serviço DNS para o domínio de e-mail que você adicionou à Amazon WorkMail, migre o serviço DNS do domínio para o Route 53. Para ter mais informações, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente.
2. Adicione uma WorkMail organização e um domínio de e-mail da Amazon. Para obter mais informações, consulte Conceitos básicos para novos usuários no Amazon WorkMail Administrator Guide.

Para criar um registro TXT do Route 53 para a Amazon WorkMail

1. No painel de navegação do WorkMail console da Amazon, escolha Domínios.
2. Escolha o nome do domínio de e-mail, como example.com, que você deseja usar para rotear o tráfego para a Amazon. WorkMail

3. Em uma nova guia do navegador, abra o console do Route 53.
4. No console do Route 53, faça o seguinte:
   a. No painel de navegação, escolha Zonas hospedadas.
   b. Escolha o nome da zona hospedada que você deseja usar para o seu domínio de WorkMail e-mail da Amazon.
5. No WorkMail console da Amazon, na seção Etapa 1: Verificar a propriedade do domínio, acesse a coluna Hostname e copie a parte do valor que precede seu nome de domínio de e-mail.

   Por exemplo, se seu domínio de WorkMail e-mail da Amazon for example.com e o valor de Hostname for _amazonses.example.com, copie _amazonses.
6. No console do Route 53, faça o seguinte:
   a. Escolha Create record (Criar registro) e escolha Simple routing (Roteamento simples).
   b. Para Record name (Nome do registro), cole o valor que você copiou na etapa 5.
   c. Para Record type (Tipo de registro), escolha TXT - Text (TXT - Texto).
7. No WorkMail console da Amazon, para o registro TXT, copie o valor da coluna Valor, incluindo as aspas.
8. No console do Route 53, faça o seguinte:
   a. Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha o endereço IP ou outro valor dependendo do tipo de registro e cole o valor que você copiou na etapa 7.

      Não altere nenhuma outra configuração.
   b. Selecione Create (Criar).

Para criar um registro MX do Route 53 para a Amazon WorkMail

1. No WorkMail console da Amazon, na seção Etapa 2: finalizar a configuração do domínio, vá até a linha que tem um tipo de registro de MX e copie o valor da coluna Valor.
2. No console do Route 53, faça o seguinte:
   a. Escolha Create record (Criar registro).
   b. Para Value/Route traffic to (Valor/Encaminhar tráfego para, escolha o endereço IP ou outro valor dependendo do tipo de registro e cole o valor que você copiou na etapa 1.

c. Para Record type (Tipo de registro), escolha MX – Mail Exchange (MX - Servidor de mensagens).

   Não altere nenhuma outra configuração.

d. Escolha Create records (Criar registros).

Para criar quatro registros CNAME do Route 53 para a Amazon WorkMail

1. No WorkMail console da Amazon, na seção Etapa 2: finalizar a configuração do domínio, vá para a primeira linha que tem um tipo de registro de CNAME. Na coluna Nome do host, copie a parte do valor que precede o nome de domínio do seu e-mail.

   Por exemplo, se seu domínio de WorkMail e-mail da Amazon for example.com e o valor de Hostname for autodiscover.example.com, copie autodiscover.

2. No console do Route 53, faça o seguinte:

   a. Escolha Create record (Criar registro).
   b. Para Record name (Nome do registro), cole o valor que você copiou na etapa 1.
   c. Para Record type (Tipo de registro), escolha CNAME – Canonical Name (CNAME - Nome canônico).

3. No WorkMail console da Amazon, na primeira linha que tem um tipo de registro de CNAME, copie o valor da coluna Valor.
4. No console do Route 53, faça o seguinte:

   a. Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha endereço IP ou outro valor dependendo do tipo de registro e cole o valor que você copiou na etapa 3.

      Não altere nenhuma outra configuração.

   b. Escolha Create records (Criar registros).

5. Repita as etapas de 1 a 4 para os registros CNAME restantes listados no WorkMail console da Amazon.

Roteamento de tráfego para outros recursos AWS

Segue uma lista de tópicos em outros guias sobre como utilizar o Route 53 para rotear o tráfego para esses serviços.

- Usar o AWS Cloud Map, no Guia do usuário do AWS Cloud Map .
- Gerencie domínios personalizados no Guia do AWS App Runner desenvolvedor.
- Usar o Route 53 como provedor de DNS, no Guia do usuário do AWS Transfer Family .
- Usar o Route 53 para apontar um domínio para uma instância do Amazon Lightsail.

Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS

As verificações de integridade do Amazon Route 53 monitoram a integridade e a performance das suas aplicações Web, servidores Web e outros recursos. Cada verificação de integridade que você criar pode monitorar um dos seguintes:

- A integridade de um recurso especificado, como um servidor Web
- O status de outras verificações de integridade.
- O status de um CloudWatch alarme da Amazon.
- Além disso, com o Amazon Route 53 Application Recovery Controller, você pode configurar verificações de integridade do controle de roteamento com registros de failover de DNS para gerenciar o failover de tráfego para sua aplicação. Para saber mais, consulte Guia do desenvolvedor do Amazon Route 53 Application Recovery Controller.

Para obter uma visão geral dos três tipos de verificações de integridade, consulte Tipos de verificações de integridade do Amazon Route 53. Para obter informações sobre como criar verificações de integridade, consulte Criar e atualizar verificações de integridade.

Depois de criar uma verificação de integridade, você poderá ver o status dela, receber notificações quando houver alteração de status e configurar o failover de DNS:

Ver o status e as notificações das verificações de integridade

Você pode visualizar os status atual e recente das suas verificações de integridade no console do Route 53. Você também pode trabalhar com verificações de saúde programaticamente por meio de um dos AWS SDKs, do AWS Command Line Interface AWS Tools for Windows PowerShell, ou da API do Route 53.

Se você quiser receber uma notificação quando o status de uma verificação de saúde mudar, você pode configurar um CloudWatch alarme da Amazon para cada verificação de saúde.

Para obter informações sobre como visualizar o status da verificação de integridade e receber notificações, consulte Monitorar o status da verificação de integridade e receber notificações.

Configurar failover de DNS

Se houver vários recursos executando a mesma função, você poderá configurar o failover de DNS para que o Route 53 encaminhe seu tráfego de um recurso não íntegro para um recurso íntegro. Por exemplo, se houver dois servidores da Web e um deles se tornar não íntegro, o Route 53 poderá encaminhar o tráfego dele para outro servidor da Web. Para ter mais informações, consulte Configurar failover de DNS.

Tópicos

Tipos de verificações de integridade do Amazon Route 53

É possível criar os seguintes tipos de verificações de integridade do Amazon Route 53:

Verificações de integridade que monitoram um endpoint

É possível configurar uma verificação de integridade que monitora um endpoint que você especificou por endereço IP ou por nome de domínio. Em intervalos regulares que você especifica, o Route 53 envia solicitações automatizadas pela Internet para sua aplicação, servidor ou outro recurso, a fim de verificar se está acessível, disponível e funcional. Se preferir, você pode configurar a verificação de integridade para fazer solicitações semelhantes àquelas que seus usuários fazem, por exemplo, solicitação de uma página da web a partir de um URL específico.

Verificações de integridade que monitoram outras verificações de integridade (verificações de integridade calculadas)

É possível criar uma verificação de integridade que monitora se outras verificações de integridade são íntegras ou não íntegras segundo o Route 53. Isso pode ser útil quando houver vários

recursos executando a mesma função (por exemplo, vários servidores da web), e sua principal preocupação for garantir uma quantidade mínima de recursos íntegros. É possível criar uma verificação de integridade para cada recurso sem ter que configurar notificações para essas verificações de integridade. Em seguida, você poderá criar uma verificação de integridade que monitore o status das outras verificações de integridade e avise somente quando a quantidade disponível de recursos da web estiver abaixo de um limite especificado.

Verificações de saúde que monitoram CloudWatch alarmes

Você pode criar CloudWatch alarmes que monitorem o status das CloudWatch métricas, como o número de eventos de leitura limitados para um banco de dados do Amazon DynamoDB ou o número de hosts do Elastic Load Balancing considerados íntegros. Depois de criar um alarme, você pode criar uma verificação de saúde que monitore o mesmo fluxo de dados que CloudWatch monitora o alarme.

Para melhorar a resiliência e a disponibilidade, o Route 53 não espera que o CloudWatch alarme entre no `ALARM` estado. O status de uma verificação de saúde muda de íntegro para não íntegro com base no fluxo de dados e nos critérios do CloudWatch alarme.

O Route 53 suporta CloudWatch alarmes com os seguintes recursos:

- Métricas de resolução padrão. As métricas de alta resolução não são compatíveis. Para obter mais informações, consulte Métricas de alta resolução no Guia do CloudWatch usuário da Amazon.
- Estatísticas: Média, Mínimo, Máximo, Soma SampleCount e. As estatísticas Extended não são compatíveis.
- Uma verificação de saúde só pode monitorar um CloudWatch alarme que exista na mesma AWS conta da verificação de saúde.

Amazon Route 53 Application Recovery Controller

O Amazon Route 53 Application Recovery Controller fornece informações sobre se suas aplicações e recursos estão prontos para recuperação e ajuda a gerenciar e coordenar o failover. As verificações de integridade no Route 53 ARC estão associadas a controles de roteamento, que são interruptores liga/desliga simples. Você configura cada verificação de integridade do controle de roteamento com um registro DNS de failover. Em seguida, você pode simplesmente atualizar seus controles de roteamento no Route 53 ARC para redirecionar o tráfego e fazer o failover de seus aplicativos, por exemplo, entre zonas de disponibilidade ou regiões. AWS Para obter mais informações, consulte Guia do desenvolvedor do Amazon Route 53 Application Recovery Controller.

Para saber mais sobre verificações de preparação, consulte Verificação de preparação no Route 53 ARC, e para saber mais sobre controles de roteamento, consulte Routing control in Route 53 ARC (Controle de roteamento no Route 53 ARC) no Guia do desenvolvedor do Route 53 ARC.

Como o Amazon Route 53 determina a integridade de uma verificação de integridade

O método que o Amazon Route 53 usa para determinar se a verificação de integridade é íntegra, depende do tipo de verificação de integridade.

Tópicos

Como o Route 53 determina o status das verificações de integridade que monitoram um endpoint

O Route 53 tem verificadores de integridade em vários locais em todo o mundo. Quando você cria uma verificação de integridade que monitora um endpoint, os verificadores de integridade começam a enviar solicitações para o endpoint especificado a fim de determinar se ele é íntegro. Você pode escolher os locais que deseja que o Route 53 use, além de especificar o intervalo entre as verificações: a cada 10 ou 30 segundos. Observe que os verificadores de integridade do Route 53 em diferentes datacenters não se coordenam entre si. Por isso, haverá várias solicitações por segundo, independentemente do intervalo escolhido, seguidas por alguns segundos, sem quaisquer verificações de integridade.

Cada verificador avalia a integridade do endpoint com base em dois valores:

- Tempo de resposta. Um recurso pode estar lento ou pode não responder a uma solicitação de verificação de integridade por vários motivos. Por exemplo, o recurso é desativado para manutenção, sob um ataque DDoS (distributed denial of service, ataques distribuídos de negação de serviço), ou a rede está desativada.

- Se o endpoint responde ou não a um número de verificações de integridade consecutivas especificado por você (o limite de falha)

O Route 53 agrega os dados dos verificadores de integridade e determina se o endpoint é íntegro:

- Se mais de 18% dos verificadores de integridade identificam um endpoint como íntegro, o Route 53 o considera íntegro.
- Se 18% ou menos verificadores de integridade identificam um endpoint como íntegro, o Route 53 o considera como não íntegro.

O valor de 18% foi escolhido para garantir que os verificadores de integridade de várias regiões consideram o endpoint como íntegro. Isso evita que um endpoint seja considerado não íntegro apenas porque as condições de rede isolaram o endpoint de algumas localizações de verificação de integridade. Esse valor pode ser alterado em versões futuras.

O tempo de resposta que um verificador de integridade individual usa para determinar se um endpoint é íntegro depende do tipo de verificação:

- Verificações de integridade HTTP e HTTPS: o Route 53 precisa estabelecer uma conexão TCP com o endpoint em quatro segundos. Além disso, o endpoint precisa responder com um código de status HTTP igual ou superior a 2xx ou 3xx dentro de dois segundos após a conexão.

  > **Note**
  >
  > As verificações de integridade HTTPS não validam certificados SSL/TLS, portanto, as verificações não falham se um certificado for inválido ou tiver expirado.

- Verificações de integridade TCP: o Route 53 deve estabelecer uma conexão TCP com o endpoint em dez segundos.
- Verificações de integridade HTTP e HTTPS com correspondência de string: como em verificações de integridade HTTP e HTTPS, o Route 53 deve estabelecer uma conexão TCP com o endpoint em quatro segundos, e o endpoint precisa responder com um código de status HTTP igual ou superior a 2xx ou 3xx dentro de dois segundos após a conexão.

  Depois que um verificador de integridade do Route 53 recebe o código de status HTTP, ele deve receber o corpo de resposta do endpoint nos próximos dois segundos. O Route 53 pesquisa no corpo da resposta a string que você especificou. A string precisa aparecer completamente

nos primeiros 5.120 bytes do corpo da resposta. Caso contrário, a verificação de integridade do endpoint falhará. Se estiver usando o console do Route 53, especifique a string no campo Search String (String de pesquisa). Se estiver usando a API do Route 53, especifique a string no elemento `SearchString` ao criar a verificação de integridade.

Para verificações de integridade que monitoram um endpoint (exceto verificações de integridade TCP), se a resposta do endpoint incluir cabeçalhos, os cabeçalhos devem estar no formato definido em RFC7230, Hypertext Transfer Protocol (HTTP/1.1): sintaxe e roteamento de mensagens, seção 3.2, "Campos do cabeçalho".

O Route 53 considera que a nova verificação de integridade está íntegra até que haja dados suficientes para determinar o status real: íntegro ou não íntegro. Se você escolheu a opção de inverter o status da verificação de integridade, o Route 53 considera que a nova verificação de integridade é não íntegra até que haja dados suficientes.

Como o Route 53 determina o status das verificações de integridade que monitoram outras verificações de integridade

Uma verificação de integridade pode monitorar o status de outras verificações de integridade. Esse tipo de verificação é conhecido como verificação de integridade calculada. A verificação de integridade que faz o monitoramento é a verificação de integridade principal, e a que é monitorada é a verificação de integridade filha. Uma verificação de integridade principal pode monitorar a integridade de até 255 verificações de integridade secundárias. Veja como o monitoramento funciona:

- O Route 53 soma o número de verificações de integridade filha consideradas íntegras.
- O Route 53 compara esse número com o número de verificações de integridade dependentes que precisam ser íntegras para que o status da verificação de integridade principal também seja íntegro.

Para obter mais informações, consulte Monitorar outras verificações de integridade (calculadas) em Valores que você especifica quando cria ou atualiza uma verificação de integridade.

O Route 53 considera que a nova verificação de integridade está íntegra até que haja dados suficientes para determinar o status real: íntegro ou não íntegro. Se você escolheu a opção de inverter o status da verificação de integridade, o Route 53 considera que a nova verificação

de integridade é não íntegra até que haja dados suficientes. Se você inverter a verificação de integridade, o Route 53 tratará um endpoint íntegro como não íntegro e vice-versa.

Como o Route 53 determina o status das verificações de saúde que monitoram os CloudWatch alarmes

Quando você cria uma verificação de saúde baseada em um CloudWatch alarme, o Route 53 monitora o fluxo de dados do alarme correspondente em vez de monitorar o estado do alarme. Se o streaming de dados indicar que o estado do alarme é OK, a verificação será considerada íntegra. Se o streaming de dados indicar que o estado é Alarme, a verificação será considerada não íntegra. Se o streaming de dados não fornecer informações suficientes para determinar o estado do alarme, o status da verificação dependerá da configuração do Status da verificação de integridade: íntegra, não íntegra ou último status conhecido. (Na API do Route 53, essa configuração é `InsufficientDataHealthStatus`.)

O Route 53 não oferece suporte a alarmes entre contas CloudWatch .

> **Note**
>
> Como as verificações de saúde do Route 53 monitoram fluxos de CloudWatch dados em vez do estado dos CloudWatch alarmes, você não pode forçar a alteração do status de uma verificação de saúde usando a operação da API CloudWatch SetAlarmState.

O Route 53 considera que a nova verificação de integridade está íntegra até que haja dados suficientes para determinar o status real: íntegro ou não íntegro. Se você escolheu a opção de inverter o status da verificação de integridade, o Route 53 considera que a nova verificação de integridade é não íntegra até que haja dados suficientes. Se você inverter a verificação de integridade, o Route 53 tratará um endpoint íntegro como não íntegro e vice-versa.

Criar, atualizar e excluir verificações de integridade

Os procedimentos nos tópicos a seguir explicam como criar, atualizar e excluir verificações de integridade do Route 53.

> **Important**
>
> Se estiver atualizando ou excluindo verificações de integridade associadas a registros, revise as tarefas em Atualizar ou excluir verificações de integridade quando o failover de DNS estiver configurado antes de continuar.

Tópicos

Criar e atualizar verificações de integridade

O procedimento a seguir descreve como criar e atualizar verificações de integridade usando o console do Route 53.

Para criar ou atualizar uma verificação de integridade (console)

1. Se estiver atualizando verificações de integridade já associadas a registros, realize as tarefas recomendadas em Atualizar ou excluir verificações de integridade quando o failover de DNS estiver configurado.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, selecione Verificações de integridade.
4. Se você quiser atualizar uma verificação de integridade existente, selecione-a e, em seguida, escolha a opção Editar verificação de integridade.

Se você deseja criar uma verificação de integridade, selecione Criar verificação de integridade. Para obter mais informações sobre cada configuração, posicione o ponteiro do mouse sobre um rótulo para ver a dica de ferramenta dele.

5. Insira os valores aplicáveis. Observe que alguns valores não podem ser alterados depois de criar uma verificação de integridade. Para ter mais informações, consulte Valores que você especifica quando cria ou atualiza uma verificação de integridade.
6. Selecione Criar verificação de integridade.

> **Note**
>
> O Route 53 considera que a nova verificação de integridade está íntegra até que haja dados suficientes para determinar o status real: íntegro ou não íntegro. Se você escolheu a opção de inverter o status da verificação de integridade, o Route 53 considera que a nova verificação de integridade é não íntegra até que haja dados suficientes.

7. Associe a verificação de integridade a um ou mais registros do Route 53. Para obter mais informações sobre como criar e atualizar registros, consulte Trabalhar com registros.

Valores que você especifica quando cria ou atualiza uma verificação de integridade

Ao criar ou atualizar verificações de integridade, você deve especificar os valores aplicáveis. Observe que alguns valores não podem ser alterados depois de criar uma verificação de integridade.

Tópicos

- Monitorar um endpoint
- Monitorar outras verificações de integridade (calculadas)
- Monitorar um alarme do CloudWatch
- Configuração avançada (somente a opção "Monitorar um endpoint")
- Receber notificação quando uma verificação de integridade apresentar falha

Nome

Opcional, mas recomendável: o nome que você deseja atribuir à verificação de integridade. Se você especificar um valor para Name (Nome), o Route 53 adicionará uma tag à verificação de integridade, atribuirá o valor Name (Nome) à chave da tag e atribuirá o valor especificado ao valor da tag. O valor da tag Name (Nome) é exibido na lista de verificações de integridade, no console do Route 53. Com isso, é possível distinguir facilmente as verificações de integridade umas das outras.

Para obter mais informações sobre a adição de tags e as verificações de integridade, consulte Nomear e adicionar tags às verificações de integridade.

O que monitorar

Se você quiser que esta verificação de integridade monitore um endpoint ou o status de outras verificações de integridade:

- Endpoint: o Route 53 monitora a integridade de um endpoint especificado por você. Você pode especificar o endpoint fornecendo um nome de domínio ou um endereço IP e uma porta.

  > **Note**
  >
  > Se você especificar um AWS ponto não final, será aplicada uma taxa adicional. Para obter mais informações, incluindo uma definição dos endpoints da AWS , consulte "Verificações de integridade" na página Preços do Route 53.

- Status de outras verificações de integridade (verificação de integridade calculada): o Route 53 determina se a verificação de integridade em questão é íntegra com base no status de outras verificações de integridade que você especificou. Você também especifica quantas verificações de integridade precisam ser consideradas íntegras para que a verificação de integridade em questão também seja.
- Estado do fluxo de dados do CloudWatch alarme — O Route 53 determina se essa verificação de saúde está íntegra monitorando o fluxo de dados de um CloudWatch alarme.

Monitorar um endpoint

Se você quiser que a verificação de integridade em questão monitore um endpoint, especifique os seguintes valores:

- Specify endpoint by

- Protocol
- IP address
- Host name
- Port
- Domain name
- Path

Especificar endpoint por

Se você quiser especificar o endpoint usando um endereço IP ou um nome de domínio.

Após criar uma verificação de integridade, não é possível alterar o valor de Especificar endpoint por.

Protocol (Protocolo)

O método que você deseja que o Route 53 utilize para verificar a integridade do seu endpoint:

- HTTP: o Route 53 tenta estabelecer uma conexão TCP. Se a conexão for bem-sucedida, o Route 53 enviará uma solicitação HTTP e aguardará o recebimento de um código de status HTTP de 2xx ou 3xx.
- HTTPS: o Route 53 tenta estabelecer uma conexão TCP. Se a conexão for bem-sucedida, o Route 53 enviará uma solicitação HTTP e aguardará o recebimento de um código de status HTTPS de 2xx ou 3xx.

> **Important**
>
> Se você escolher HTTPS, o endpoint deverá ser compatível com TLS v1.0, v1.1 ou v1.2.

Se você escolher HTTPS como valor de Protocolo, uma taxa adicional será cobrada. Para obter mais informações, consulte Preço do Route 53.

- TCP: o Route 53 tenta estabelecer uma conexão TCP.

Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Após criar uma verificação de integridade, não é possível alterar o valor de Protocolo.

Endereço IP (somente a opção "Especificar endpoint por endereço IP")

O endereço IPv4 ou IPv6 do endpoint no qual você deseja que o Route 53 faça verificações de integridade, caso tenha escolhido a opção Specify endpoint by IP address (Especificar endpoint por endereço IP).

O Route 53 não pode verificar a integridade dos endpoints cujos endereços IP estejam em intervalos locais, privados, não roteáveis ou multicast. Para obter mais informações sobre endereços IP cuja integridade não pode ser verificada, consulte os seguintes documentos:

- RFC 5735, Special Use IPv4 Addresses (RFC 5735, Endereços IPv4 de uso especial)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space. (RFC 6598, Prefixo IPv4 reservado por IANA para espaço de endereço compartilhado.)
- RFC 5156, Special-Use IPv6 Addresses (RFC 5156, Endereços IPv6 de uso especial)

Se o endpoint for uma instância do Amazon EC2, recomendamos criar um endereço de IP elástico, associar ele à sua instância do EC2 e o especificar o endereço de IP elástico. Isso garante que o endereço IP da sua instância permaneça sempre o mesmo. Para obter mais informações, consulte Endereços IP elásticos (EIP) no Guia do usuário do Amazon EC2.

Se você excluir a instância do Amazon EC2, certifique-se de excluir também a verificação de integridade associada ao EIP. Para ter mais informações, consulte Práticas recomendadas para endereços de IP elástico para verificações de integridade.

> **Note**
>
> Se você especificar um AWS ponto não final, será aplicada uma taxa adicional. Para obter mais informações, incluindo uma definição dos endpoints da AWS , consulte “Verificações de integridade” na página Preços do Route 53.

Nome de host (somente a opção "Especificar endpoint por endereço IP" e somente protocolos HTTP e HTTPS)

O valor que você deseja que o Route 53 passe no cabeçalho `Host` nas verificações de integridade de HTTP e HTTPS. Normalmente, esse é o nome de DNS totalmente qualificado do site em que você deseja que o Route 53 faça as verificações de integridade. Quando o Route 53 verifica a integridade de um endpoint, o cabeçalho `Host` é criado desta forma:

- Se você especificar o valor de **80** para Port (Porta) e HTTP para Protocol (Protocolo), o Route 53 passará para o endpoint um cabeçalho `Host` contendo o valor de Host name (Nome do host).
- Se você especificar o valor de **443** para Port (Porta) e HTTPS para Protocol (Protocolo), o Route 53 passará para o endpoint um cabeçalho `Host` contendo o valor de Host name (Nome do host).
- Se você especificar outro valor para Port (Porta) e HTTP ou HTTPS para Protocol (Protocolo), o Route 53 passará ao endpoint um cabeçalho `Host` contendo o valor *`Host name`* (Nome do host) :*`Port`* (Porta).

Se você optar por especificar o endpoint por endereço IP e não especificar um valor para Host name (Nome do host), o Route 53 substituirá o valor de IP address (Endereço IP) no cabeçalho `Host` em cada um dos casos anteriores.

Port (Porta)

A porta no endpoint no qual você deseja que o Route 53 faça as verificações de integridade.

Nome de domínio (somente a opção "Especificar endpoint por nome de domínio", todos os protocolos)

O nome do domínio (example.com) ou o nome do subdomínio (back-end.example.com) do endpoint no qual você deseja que o Route 53 faça verificações de integridade, caso tenha escolhido a opção Specify endpoint by domain name (Especificar endpoint por nome de domínio).

Se você optar por especificar o endpoint por nome de domínio, o Route 53 enviará uma consulta de DNS para resolver o nome do domínio que você especificou em Domain name (Nome do domínio) no intervalo definido em Request interval (Intervalo de solicitações). Usando um endereço IP que o DNS retorna, o Route 53 verifica a integridade do endpoint.

> **Note**
>
> Se você especificar o endpoint por nome de domínio, o Route 53 usará somente o IPv4 para enviar verificações de integridade ao endpoint. Se não houver nenhum registro com um tipo de A para o nome que você especifica para Domain name, a verificação de integridade falhará e exibirá o erro "DNS resolution failed".

Se desejar verificar a integridade dos registros ponderados, de geolocalização, de geoproximity, de latência ou de failover e tiver especificado o endpoint pelo nome de domínio, recomendamos

criar uma verificação de integridade separada para cada endpoint. Por exemplo, crie uma verificação de saúde para cada servidor HTTP que esteja veiculando conteúdo para www.example.com. Para o valor Domain name, especifique o nome do domínio do servidor (como us-east-2-www.example.com), não o nome dos registros (www.example.com).

> **Important**
>
> Nessa configuração, se você criar uma verificação de integridade para a qual o valor de Domain name corresponde ao nome dos registros e, em seguida, associar a verificação de integridade a esses registros, os resultados da verificação de integridade serão imprevisíveis.

Além disso, se o valor de Protocol (Protocolo) for HTTP ou HTTPS, o Route 53 passará o valor de Domain name (Nome de domínio) no cabeçalho `Host`, conforme descrito em Host name (Nome do host), anteriormente nesta lista. Se o valor de Protocol (Protocolo) for TCP, o Route 53 não passará um cabeçalho `Host`.

> **Note**
>
> Se você especificar um AWS ponto não final, será aplicada uma taxa adicional. Para obter mais informações, incluindo uma definição dos endpoints da AWS , consulte "Verificações de integridade" na página Preços do Route 53.

Caminho (somente protocolos HTTP e HTTPS)

O caminho que você deseja que o Route 53 solicite ao executar verificações de integridade. O caminho pode ser qualquer valor para o qual o endpoint retorna um código de status HTTP de `2xx` ou `3xx` quando o endpoint é íntegro, como o arquivo `/docs/route53-health-check.html`. Você também pode incluir parâmetros de strings de consulta, por exemplo, `/welcome.html?language=jp&login=y`. Se você não incluir uma barra inicial (`/`), o Route 53 adicionará uma automaticamente.

Monitorar outras verificações de integridade (calculadas)

Se você quiser que esta verificação de integridade monitore o status de outras verificações de integridade, especifique os valores a seguir:

- Health checks to monitor
- Report healthy when
- Invert health check status
- Disabled

Verificações de integridade a serem monitoradas

As verificações de integridade que você deseja que o Route 53 monitore para verificar se uma determinada verificação de integridade é íntegra.

Você pode adicionar até 256 verificações de integridade às Verificações de integridade a serem monitoradas. Para remover uma verificação de integridade da lista, clique em x à direita da verificação em questão.

> **Note**
>
> Não é possível configurar uma verificação de integridade calculada para monitorar a integridade de outras verificações de integridade calculadas.

Se você desabilitar uma verificação de integridade que uma verificação de integridade calculada esteja monitorando, o Route 53 considera a verificação de integridade desabilitada como íntegra à medida que calcula se a verificação de integridade é íntegra. Se você quiser que a verificação de integridade desabilitada seja considerada não íntegra, marque a caixa de seleção Invert health check status (Inverter status da verificação de integridade).

Informar como íntegra quando

O cálculo que você deseja que o Route 53 use para determinar se a verificação de integridade é íntegra:

- Relatar como íntegra quando pelo menos x de y verificações de integridade selecionadas estiverem íntegras: o Route 53 considera a verificação de integridade como íntegra quando uma quantidade especificada de verificações de integridade que você adicionou às Verificações de integridade a serem monitoradas for íntegra. Observe o seguinte:
  - Se você especificar uma quantidade maior que a quantidade de verificações de integridade em Verificações de integridade a serem monitoradas o Route 53 sempre considerará essa verificação de integridade como não íntegra.

- Se você especificar 0, o Route 53 sempre considerará essa verificação de integridade como íntegra.

- Relatar como íntegra quando todas as verificações de integridade estiverem íntegras (E): o Route 53 considera a verificação de integridade como íntegra somente quando todas as verificações de integridade que você adicionou às Verificações de integridade a serem monitoradas estiverem íntegras.
- Relatar como íntegra quando uma ou mais verificações de integridade estiverem íntegras (OU): o Route 53 considera a verificação de integridade como íntegra quando pelo menos uma das verificações de integridade que você adicionou às Verificações de integridade a serem monitoradas estiver íntegra.

Inverter status da verificação de integridade

Informe se você deseja que o Route 53 inverta o status de uma verificação de integridade. Se você escolher essa opção, o Route 53 considerará as verificações de integridade como não íntegras quando o status for íntegro e vice-versa.

desabilitados

Impede o Route 53 de executar verificações de integridade. Quando você desabilitar uma verificação de integridade, o Route 53 deixará de agregar o status das verificações de integridade referenciadas.

Depois de desativar uma verificação de integridade, o Route 53 considerará o status da verificação de integridade como sendo sempre íntegra. Se você configurar o failover de DNS, o Route 53 continuará encaminhando o tráfego para os recursos correspondentes. Se você deseja interromper o roteamento do tráfego para um recurso, altere o valor de Invert health check status.

> **Note**
>
> Cobranças para uma verificação de integridade ainda serão aplicáveis quando a verificação de integridade estiver desabilitada.

Monitorar um alarme do CloudWatch

Se você quiser que essa verificação de integridade monitore o estado de alarme de um CloudWatch alarme, especifique os seguintes valores:

- CloudWatch alarm

- Health check status
- Invert health check status
- Disabled

CloudWatch alarme

Escolha o CloudWatch alarme que você deseja que o Route 53 use para determinar se essa verificação de saúde está íntegra. O CloudWatch alarme deve ser Conta da AWS igual ao da verificação de saúde.

> **Note**
>
> O Route 53 suporta CloudWatch alarmes com os seguintes recursos:
>
> - Métricas de resolução padrão. As métricas de alta resolução não são compatíveis. Para obter mais informações, consulte Métricas de alta resolução no Guia do CloudWatch usuário da Amazon.
> - Estatísticas: `Average`, `Minimum`, `Maximum`, `Sum` e `SampleCount`. As estatísticas Extended não são compatíveis.
> - O Route 53 não suporta alarmes “M out of N” (M de N). Para obter mais informações, consulte Avaliação de um alarme no CloudWatch guia da Amazon.
>
> O Route 53 não oferece suporte a alarmes que usam matemática métrica para consultar várias CloudWatch métricas.

Se você quiser criar um alarme, siga estas etapas:

1. Escolha Create (Criar). O CloudWatch console aparece em uma nova guia do navegador.
2. Insira os valores aplicáveis. Para obter mais informações, consulte Criar ou editar um CloudWatch alarme no Guia do CloudWatch usuário da Amazon.
3. Retorne para a guia do navegador em que o console do Route 53 foi exibido.
4. Escolha o botão de atualização ao lado da lista de CloudWatchalarmes.
5. Escolha o novo alarme na lista.

> **Important**
>
> Se você alterar as configurações do CloudWatch alarme depois de criar uma verificação de saúde, deverá atualizá-la. Para ter mais informações, consulte Atualizar verificações de saúde ao alterar as configurações de CloudWatch alarme (verificações de saúde que monitoram somente um CloudWatch alarme).

Status da verificação de integridade

Escolha o status da verificação de saúde (íntegro, não íntegro ou último status conhecido) quando CloudWatch tiver dados insuficientes para determinar o estado do alarme que você escolheu para o CloudWatchalarme. Se você optar por usar o último status conhecido, o Route 53 usa o status da verificação de saúde da última vez que CloudWatch tinha dados suficientes para determinar o estado do alarme. Para novas verificações de integridade que não têm último status conhecido, o status padrão indicará a integridade como íntegra.

O valor de Health check status fornece um status temporário quando o fluxo de dados de uma CloudWatch métrica está brevemente indisponível. (O Route 53 monitora os fluxos de dados em busca de CloudWatch métricas, não o estado do alarme correspondente.) Se a métrica estará indisponível com frequência ou por longos períodos (mais do que algumas horas), recomendamos não usar o último status conhecido.

Inverter status da verificação de integridade

Informe se você deseja que o Route 53 inverta o status de uma verificação de integridade. Se você escolher essa opção, o Route 53 considerará as verificações de integridade como não íntegras quando o status for íntegro e vice-versa.

desabilitados

Impede o Route 53 de executar verificações de integridade. Quando você desativa uma verificação de saúde, o Route 53 para de monitorar as CloudWatch métricas correspondentes.

Depois de desativar uma verificação de integridade, o Route 53 considerará o status da verificação de integridade como sendo sempre íntegra. Se você configurar o failover de DNS, o Route 53 continuará encaminhando o tráfego para os recursos correspondentes. Se você deseja interromper o roteamento do tráfego para um recurso, altere o valor de Invert health check status.

> **Note**
>
> Cobranças para uma verificação de integridade ainda serão aplicáveis quando a verificação de integridade estiver desabilitada.

Configuração avançada (somente a opção "Monitorar um endpoint")

Se você optar por monitorar um endpoint, também poderá especificar as seguintes configurações:

- Request interval
- Failure threshold
- String matching
- Search string
- Latency graphs
- Enable SNI
- Health checker regions
- Invert health check status
- Disabled

Intervalo de solicitações

A quantidade de segundos entre o momento em que cada verificador de integridade do Route 53 obtém uma resposta do seu endpoint e o momento em que ele envia a próxima solicitação de verificação de integridade. Se você escolher um intervalo de 30 segundos, cada um dos verificadores de integridade do Route 53 nos datacenters em todo o mundo enviará uma solicitação de verificação de integridade ao seu endpoint a cada 30 segundos. Em média, seu endpoint receberá uma solicitação de verificação de integridade a cada dois segundos. Se você escolher um intervalo de 10 segundos, o endpoint receberá mais de uma solicitação por segundo.

Observe que os verificadores de integridade do Route 53 em diferentes datacenters não se coordenam entre si. Por isso, haverá várias solicitações por segundo, independentemente do intervalo escolhido, seguidas por alguns segundos, sem quaisquer verificações de integridade.

Após criar uma verificação de integridade, não é possível alterar o valor do Intervalo de solicitações.

> **Note**
>
> Se você escolher Rápido (10 segundos) como valor de Intervalo de solicitações, uma taxa adicional será cobrada. Para obter mais informações, consulte Preço do Route 53.

Limite de falha

A quantidade de verificações de integridade consecutivas pelas quais um endpoint precisa passar para que o Route 53 altere o status atual de integridade de um endpoint de não íntegro para íntegro ou vice-versa. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Correspondência de string (somente HTTP e HTTPS)

Se você quiser que o Route 53 determine a integridade de um endpoint enviando uma solicitação HTTP ou HTTPS para ele e pesquisando uma determinada string no corpo da resposta. Se o corpo da resposta contiver o valor especificado em Search string (String de pesquisa), o Route 53 considerará o endpoint como íntegro. Caso contrário, ou se o endpoint não retornar uma resposta, o Route 53 considerará o endpoint como não íntegro. A string de pesquisa precisa aparecer completa nos primeiros 5.120 bytes do corpo da resposta.

Após criar uma verificação de integridade, não é possível alterar o valor de Correspondência de string.

> **Note**
>
> Se você escolher Sim como valor de Correspondência de string, uma taxa adicional será cobrada. Para obter mais informações, consulte Preço do Route 53.

Como os verificadores de integridade lidam com uma resposta compactada

Se o endpoint for um servidor Web que retorna uma resposta compactada, o verificador de integridade do Route 53 descompactará a resposta antes de verificar a string de pesquisa especificada somente se o servidor Web compactou a resposta usando um algoritmo de compactação compatível com os verificadores de integridade. Os verificadores de Health suportam os seguintes algoritmos de compactação:

- Gzip

- Desinflar

Se a resposta for compactada usando outro algoritmo, o verificador de integridade não poderá descompactar a resposta antes de procurar a string. Nesse caso, a pesquisa quase sempre falhará e o Route 53 considerará o endpoint não íntegro

String de pesquisa (somente quando a opção "Correspondência de string" estiver habilitada)

A string que você deseja que o Route 53 pesquise no corpo da resposta do seu endpoint. O tamanho máximo é de 255 caracteres.

O Route 53 diferencia maiúsculas e minúsculas ao pesquisar a Search string (String de pesquisa) no corpo da resposta.

Gráficos de latência

Escolha se você deseja que o Route 53 meça a latência entre os verificadores de saúde em várias AWS regiões e seu endpoint. Se você escolher essa opção, os gráficos de CloudWatch latência aparecerão na guia Latência na página Verificações de saúde no console do Route 53. Se os verificadores de integridade do Route 53 não puderem se conectar ao endpoint, o Route 53 não exibirá os gráficos de latência desse endpoint.

Após criar uma verificação de integridade, não é possível alterar o valor de Medições de latência.

> **Note**
>
> Se você configurar o Route 53 para medir a latência entre verificadores de integridade e o seu endpoint, uma taxa adicional será cobrada. Para obter mais informações, consulte Preço do Route 53.

Habilitar SNI (somente HTTPS)

Especifique se você deseja que o Route 53 envie o nome do host ao endpoint na mensagem `client_hello` durante a negociação de TLS. Isso permite que o endpoint responda à solicitação de HTTPS com o certificado SSL/TLS aplicável.

Alguns endpoints exigem que as solicitações de HTTPS incluam o nome do host na mensagem `client_hello`. Se você não habilitar o SNI, o status da verificação de integridade será `SSL alert handshake_failure`. Uma verificação de integridade também pode ter esse status por

outros motivos. Se o SNI estiver habilitado e o erro ainda for exibido, verifique a configuração de SSL/TLS no seu endpoint para saber se seu certificado é válido.

Observe os seguintes requisitos:

- O endpoint precisa ser compatível com SNI.
- O certificado SSL/TLS no seu endpoint inclui um nome de domínio no campo `Common Name` e (possivelmente) vários outros no campo `Subject Alternative Names`. Um dos nomes de domínio no certificado precisa corresponder ao valor que você especificou em Nome de host.

Regiões do verificador de integridade

Escolha se você deseja que o Route 53 verifique a integridade do endpoint usando verificadores de integridade nas regiões recomendadas ou nas regiões especificadas por você.

Se você atualizar uma verificação de integridade para remover uma região que realizava verificações de integridade, o Route 53 continuará a executar verificações a partir dessas regiões por até uma hora. Isso garante que alguns verificadores de integridade sempre verifiquem o endpoint (por exemplo, se você substituir três regiões por quatro regiões diferentes).

Se você escolher a opção Personalizar, clique em x ao lado da região que deseja remover. Clique no espaço na parte inferior da lista para adicionar novamente uma região a ela. É necessário especificar pelo menos três regiões.

Inverter status da verificação de integridade

Informe se você deseja que o Route 53 inverta o status de uma verificação de integridade. Se você escolher essa opção, o Route 53 considerará uma verificação de saúde não íntegra quando o status for íntegro e vice-versa. Por exemplo, você pode desejar que o Route 53 considere uma verificação de integridade como não íntegra se configurar a correspondência de string e o endpoint retornar um valor especificado. Para obter mais informações sobre verificações de integridade que executam a correspondência de strings, consulte String matching.

desabilitados

Impede o Route 53 de executar verificações de integridade. Quando você desabilitar uma verificação de integridade, o Route 53 deixará de tentar estabelecer uma conexão TCP com o endpoint.

Depois de desativar uma verificação de integridade, o Route 53 considerará o status da verificação de integridade como sendo sempre íntegra. Se você configurar o failover de DNS, o

Route 53 continuará encaminhando o tráfego para os recursos correspondentes. Se você deseja interromper o roteamento do tráfego para um recurso, altere o valor de Invert health check status.

> **Note**
>
> Cobranças para uma verificação de integridade ainda serão aplicáveis quando a verificação de integridade estiver desabilitada.

Receber notificação quando uma verificação de integridade apresentar falha

Use as seguintes opções para configurar a notificação por e-mail quando houver falha em uma verificação de integridade:

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

Criar alarme (somente ao criar verificações de integridade)

Especifique se você deseja criar um CloudWatch alarme padrão. Se você escolher Sim, CloudWatch enviará uma notificação do Amazon SNS quando o status desse endpoint mudar para não íntegro e o Route 53 considerar o endpoint não íntegro por um minuto.

> **Note**
>
> Se você quiser CloudWatch enviar outra notificação do Amazon SNS quando o status voltar para íntegro, você pode criar outro alarme depois de criar a verificação de saúde. Para obter mais informações, consulte Criação de CloudWatch alarmes da Amazon no Guia do CloudWatch usuário da Amazon.

Se desejar criar um alarme para uma verificação de integridade existente ou receber notificações quando o Route 53 considerar o endpoint como não íntegro por cerca de um minuto (o valor padrão), selecione a opção No (Não) e adicione um alarme depois de criar a verificação de integridade. Para ter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

Enviar notificação para (somente ao criar um alarme)

Especifique se você CloudWatch deseja enviar notificações para um tópico existente do Amazon SNS ou para um novo:

- Existing SNS topic (Tópico existente do SNS): selecione o nome do tópico na lista. O tópico deve estar na região Leste dos EUA (Norte da Virgínia).
- New SNS topic (Novo tópico do SNS): insira um nome para o tópico em Topic name (Nome do tópico) e os endereços de e-mail para os quais você deseja enviar notificações em Recipients (Destinatários). Separe os endereços usando vírgula (,), ponto e vírgula (;) ou espaço.

  O Route 53 criará o tópico na região Leste dos EUA (Norte da Virgínia).

Nome do tópico (somente ao criar um novo tópico do SNS)

Se você especificou Novo tópico do SNS, insira o nome do novo tópico.

Endereços de e-mail dos destinatários (somente ao criar um novo tópico do SNS)

Se você especificou Novo tópico do SNS, insira os endereços de e-mail para os quais você deseja enviar as notificações. Separe os nomes usando vírgula (,), ponto e vírgula (;) ou espaço.

Os valores que o Amazon Route 53 exibe quando você cria uma verificação de integridade

A página Criar verificação de integridade exibe os seguintes valores com base nos valores que você digitou:

URL

URL completo (para verificações de integridade HTTP ou HTTPS) ou endereço IP e porta (para verificações de integridade TCP) para onde o Route 53 enviará solicitações ao realizar verificações de integridade.

Tipo de verificação de integridade

Pode ser Básico ou Básico + opções adicionais com base nas configurações que você especificou para a verificação de integridade em questão. Para obter mais informações sobre definição de preço para opções adicionais, consulte Preço do Route 53.

Atualizar verificações de saúde ao alterar as configurações de CloudWatch alarme (verificações de saúde que monitoram somente um CloudWatch alarme)

Se você criar uma verificação de saúde do Route 53 que monitora o fluxo de dados de um CloudWatch alarme e depois atualizar as configurações no CloudWatch alarme, o Route 53 não atualizará automaticamente as configurações do alarme na verificação de saúde. Se quiser que a verificação de integridade passe a usar as novas configurações de alarme, você precisará atualizá-la.

> **Note**
>
> Você pode usar a API `UpdateHealthCheck` para atualizar uma verificação de integridade de maneira programática. Basta especificar os valores atuais para `AlarmIdentifier` e`Region`, e o Route 53 obterá as configurações mais recentes de CloudWatch. Para obter mais informações, consulte UpdateHealthVerifique a referência da API do Amazon Route 53.

Para atualizar uma verificação de saúde com novas configurações de CloudWatch alarme (console)

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Marque a caixa de seleção da verificação de integridade que você deseja atualizar.
4. Selecione a opção Editar verificação de integridade.

   Uma nota explica que o CloudWatch alarme da verificação de saúde foi alterado. O campo Detalhes mostra as novas configurações do alarme.
5. Selecione Save (Salvar).

Excluir verificações de integridade

Para excluir verificações de integridade, realize o procedimento a seguir.

> **Note**
>
> Se você estiver usando AWS Cloud Map e estiver configurado AWS Cloud Map para criar uma verificação de saúde do Route 53 ao registrar uma instância, não poderá usar o console do Route 53 para excluir a verificação de saúde. A verificação de integridade será excluída automaticamente quando você cancelar o registro da instância. Poderá levar várias horas para que a verificação de integridade deixe de ser exibida no console do Route 53.

Para excluir uma verificação de integridade (console)

1. Se estiver excluindo verificações de integridade associadas a registros, execute as tarefas recomendadas em Atualizar ou excluir verificações de integridade quando o failover de DNS estiver configurado.
2. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
3. No painel de navegação, selecione Verificações de integridade.
4. No painel direito, selecione as verificações de integridade que você deseja excluir.
5. Selecione Excluir verificação de integridade.
6. Escolha Yes, Delete (Sim, excluir) para confirmar.

Atualizar ou excluir verificações de integridade quando o failover de DNS estiver configurado

Para atualizar ou excluir verificações de integridade associadas a registros ou para alterar registros que tenham verificações de integridade associadas, analise como suas alterações afetarão o roteamento de consultas DNS e sua configuração de failover de DNS.

> **Important**
>
> O Route 53 não impede a exclusão de uma verificação de integridade mesmo que ela esteja associada a um ou mais registros. Se você excluir uma verificação de integridade e não atualizar os registros associados, o status futuro da verificação de integridade será imprevisível. Isso afetará o roteamento das consultas DNS na sua configuração de failover de DNS.

Para atualizar ou excluir verificações de integridade já associadas aos registros, recomendamos executar as seguintes tarefas:

1. Identifique os registros associados às verificações de integridade. Para identificar os registros associados a uma verificação de integridade, proceda de uma das seguintes maneiras:

   - Analise os registros em cada zona hospedada usando o console do Route 53. Para ter mais informações, consulte Listar registros.
   - Execute a ação de API `ListResourceRecordSets` em cada zona hospedada e analise a resposta. Para obter mais informações, consulte ListResourceRecordSetsa Referência de API do Amazon Route 53.
2. Avalie a mudança de comportamento resultante da atualização ou exclusão de verificações de integridade, ou da atualização de registros. Com base nessa avaliação, determine quais alterações precisam ser feitas.

   Para obter mais informações, consulte O que acontece quando você omite verificações de integridade?
3. Altere as verificações de integridade e os registros, conforme aplicável. Para obter mais informações, consulte os tópicos a seguir.

   - Criar e atualizar verificações de integridade
   - Editar registros
4. Exclua as verificações de integridade que você não está mais usando, se houver alguma. Para ter mais informações, consulte Excluir verificações de integridade.

Como configurar regras de roteador e firewall para as verificações de integridade do Amazon Route 53

Quando o Route 53 verifica a integridade de um endpoint, ele envia uma solicitação HTTP, HTTPS ou TCP para o endereço IP e a porta que você especificou quando criou a verificação de integridade. Para que uma verificação de integridade seja bem-sucedida, as regras do roteador e do firewall precisam permitir o tráfego de entrada dos endereços IP utilizados pelos verificadores de integridade do Route 53.

Para ver a lista atual de endereços IP dos verificadores de integridade do Route 53, dos servidores de nomes do Route 53 e de outros AWS serviços, consulteIntervalos de endereço IP dos servidores do Amazon Route 53.

No Amazon EC2, os grupos de segurança atuam como firewalls. Para obter mais informações, consulte os grupos de segurança do Amazon EC2 no Guia do usuário do Amazon EC2. Para configurar seus grupos de segurança para permitir verificações de saúde do Route 53, você pode permitir o tráfego de entrada de cada intervalo de endereços IP ou usar uma lista de prefixos gerenciada. AWS

Para usar a lista de prefixos AWS-managed, modifique seu grupo de segurança para permitir o tráfego de entrada`com.amazonaws.<region>.route53-healthchecks`, de onde `<region>` está o da sua instância ou recurso Região da AWS do Amazon EC2. Se estiver usando as verificações de integridade do Route 53 para verificar os endpoints IPv6, você também deve permitir o tráfego de entrada de `com.amazonaws.<region>.ipv6.route53-healthchecks`.

Para obter mais informações sobre listas AWS de prefixos gerenciadas, consulte Trabalhar com listas de prefixos AWS gerenciadas no Guia do usuário da Amazon VPC.

> **Important**
>
> Ao adicionar endereços IP a uma lista de endereços IP permitidos, adicione todos os endereços IP no intervalo CIDR de cada AWS região que você especificou ao criar as verificações de saúde, bem como o intervalo CIDR global. Você pode ver que solicitações de verificação de integridade vêm de apenas um endereço IP em uma região. No entanto, esse endereço IP pode ser alterado a qualquer momento para outro dos endereços IP dessa região.
>
> Se você quiser se certificar de que você inclui os endereços IP do verificador de integridade atual e mais antigos, adicione TODOS os intervalos de endereços IP /26 e /18 à lista de permissões. Para obter uma lista completa, consulte AWS IP address ranges na Referência geral da AWS.
>
> Quando você adiciona a lista de prefixos AWS-managed ao seu grupo de segurança de entrada, ela adiciona automaticamente todos os intervalos necessários.

Monitorar o status da verificação de integridade e receber notificações

É possível monitorar o status das verificações de integridade no console do Amazon Route 53. Também é possível definir alarmes do CloudWatch e receber notificações automáticas quando o status da verificação de integridade mudar.

Tópicos

Ver o status e o motivo de falhas da verificação de integridade

No console do Route 53, é possível visualizar o status (íntegro ou não íntegro) das verificações de integridade, conforme relatado pelos verificadores de integridade do Route 53. Para todas as verificações de integridade, exceto as calculadas, também é possível ver o motivo da última falha na verificação de integridade. Por exemplo, os verificadores de integridade não conseguiram estabelecer uma conexão com o endpoint.

Para ver o status e o motivo da última falha de uma verificação de integridade (console)

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Para obter uma visão geral do status de todas as suas verificações de integridade, íntegras ou não íntegras, consulte a coluna Status. Para obter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.
4. Em todas as verificações de integridade, exceto as calculadas, é possível visualizar o status dos verificadores de integridade do Route 53 que estão verificando a integridade de um endpoint especificado. Selecione a verificação de integridade.
5. No painel inferior, escolha a guia Verificadores de integridade.

> **Note**
>
> É necessário que as novas verificações de integridade se propaguem para os verificadores de integridade do Route 53 para que o status da verificação de integridade e o último motivo de falha sejam exibidos na coluna Status. Até a propagação ter terminado, a mensagem nessa coluna indica que não há nenhum status disponível.

6. Indique se você deseja visualizar o status atual da verificação de integridade ou a data/hora e o motivo da última falha. A tabela da guia Status inclui os seguintes valores:

IP do verificador de integridade

O endereço IP do verificador de integridade do Route 53 que realizou a verificação.

Última verificação

A data e a hora da verificação de integridade ou a data e hora da última falha, dependendo da opção que você selecionou na parte superior da guia Status.

Status

O status atual da verificação de integridade ou o motivo da última falha de verificação de integridade, dependendo da opção que você selecionou na parte superior da guia Status.

Monitorar a latência entre os verificadores de integridade e seu endpoint

Ao criar uma verificação de integridade, se você optar por monitorar o status de um endpoint (não o status de outras verificações de integridade) e escolher a opção Latency graphs (Gráficos de latência), os seguintes valores serão exibidos nos gráficos do CloudWatch, no console do Route 53:

- O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para estabelecer uma conexão TCP com o endpoint
- O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para receber o primeiro byte da resposta a uma solicitação HTTP ou HTTPS
- O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para concluir o handshake do SSL/TLS

> **Note**
>
> Não é possível permitir o monitoramento de latência nas verificações de integridade existentes.

> **Important**
>
> Os verificadores de integridade são executados em 16 zonas de disponibilidade redundantes. Ocasionalmente, uma zona de disponibilidade pode ficar indisponível devido

a implantações, atualizações, manutenção e assim por diante. O sistema de verificação de integridade foi projetado para levar em conta isso sem qualquer impacto no cliente.

Para visualizar a latência entre os verificadores de integridade do Route 53 e seu endpoint (console)

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Selecione as linhas para as verificações de integridade aplicáveis. Você pode visualizar dados de latência somente para verificações de integridade que monitoram status de um endpoint e para as quais a opção Gráficos de latência esteja ativada.
4. No painel inferior, escolha a guia Latência.
5. Escolha o período e a região geográfica para os quais você quer exibir os gráficos de latência.

   Os gráficos exibem o status para o período especificado:

   Tempo de conexão TCP (somente HTTP e TCP)

   O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 na região geográfica selecionada levaram para estabelecer uma conexão TCP com o endpoint.

   Tempo até o primeiro byte (somente HTTP e HTTPS)

   O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 na região geográfica selecionada levaram para receber o primeiro byte da resposta a uma solicitação HTTP ou HTTPS.

   Tempo até a conclusão do handshake do SSL (somente HTTPS)

   O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 na região geográfica selecionada levaram para concluir o handshake do SSL/TLS.

> **Note**
>
> Se você selecionar mais de uma verificação de integridade, o gráfico exibirá uma linha codificada por cores diferente para cada verificação de integridade.

6. Para visualizar um gráfico maior e especificar configurações diferentes, clique no gráfico. Você pode alterar as seguintes configurações:

   Estatística

   Altera o cálculo que o CloudWatch faz sobre os dados.

   Intervalo

   Exibe o status de uma verificação de integridade em um período diferente, por exemplo, durante a noite ou na última semana.

   Período

   Altera o intervalo entre pontos de dados no gráfico.

   Observe o seguinte:

   - Se você acabou de criar uma verificação de integridade, precisará aguardar alguns minutos para que os dados sejam exibidos no gráfico e a métrica de verificação de integridade seja exibida na lista de métricas disponíveis.
   - O gráfico não é automaticamente atualizado. Para atualizar a exibição, escolha o ícone de atualização ().
   - Se as verificações de integridade estiverem apresentando falhas por algum motivo, como tempo limite de conexão, o Route 53 não poderá medir a latência, e os dados de latência ficarão ausentes no gráfico para o período afetado.

Como monitorar as verificações de integridade usando o CloudWatch

As verificações de integridade do Route 53 se integram com as métricas do CloudWatch para que você possa fazer o seguinte:

- Averiguar se uma verificação de integridade foi configurada corretamente.
- Analisar o status de uma verificação de integridade durante um determinado período.
- Configurar o CloudWatch para enviar um alerta do Amazon SNS quando o status de uma verificação de integridade não for íntegro. Observe que vários minutos podem decorrer entre o momento em que uma verificação de integridade falha e o momento em que você recebe a notificação do SNS associado.

Para obter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

- Para visualizar o status de uma verificação de integridade (console)
- Para receber uma notificação do Amazon SNS quando um status da verificação de integridade for não íntegro (console)
- Para visualizar o status de alarme do CloudWatch e editar alarmes do Amazon Route 53 (console)
- Para visualizar as métricas do Route 53 usando o console do Amazon CloudWatch

Para visualizar o status de uma verificação de integridade (console)

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Escolha as linhas para as verificações de integridade aplicáveis.
4. No painel inferior, escolha a guia Monitoramento.

   Os dois gráficos exibem o status da última hora em intervalos de um minuto:

   Status da verificação de integridade

   O gráfico mostra a avaliação feita pelo Route 53 da integridade do endpoint. 1 indica íntegro e 0 indica não íntegro.

   Verificadores de integridade que relatam o endpoint como íntegro (%)

   Nas verificações de integridade que monitoram somente um endpoint, o gráfico mostra a porcentagem de verificadores de integridade do Route 53 que consideram o endpoint selecionado como íntegro.

   Quando a verificação de integridade está desabilitada, esta métrica não está disponível.

   Número de verificações de integridade dependentes íntegras

   Somente nas verificações de integridade calculadas, o gráfico mostra o número de verificações de integridade íntegras.

> **Note**
>
> Se você selecionou mais de uma verificação de integridade, o gráfico exibirá uma linha codificada por cores diferente para cada verificação de integridade.

5. Para visualizar um gráfico maior e especificar configurações diferentes, clique no gráfico. Você pode alterar as seguintes configurações:

   Estatística

   Altera o cálculo que o CloudWatch faz sobre os dados.

   Intervalo

   Exibe o status de uma verificação de integridade em um período diferente, por exemplo, durante a noite ou na última semana.

   Período

   Altera o intervalo entre pontos de dados no gráfico.

   Observe o seguinte:

   - Se você acabou de criar uma verificação de integridade, precisará aguardar alguns minutos para que os dados sejam exibidos no gráfico e a métrica de verificação de integridade seja exibida na lista de métricas disponíveis.
   - O gráfico não é automaticamente atualizado. Para atualizar a exibição, escolha o ícone de atualização ().

Para receber uma notificação do Amazon SNS quando um status da verificação de integridade for não íntegro (console)

1. No painel de navegação do console do Route 53, escolha Health Checks (Verificações de integridade).
2. Escolha a linha para a verificação de integridade aplicável.
3. No painel inferior, escolha a guia Alarmes.

A tabela lista os alarmes que você já criou para esta verificação de integridade.

4. Escolha Create Alarm.
5. Especifique os seguintes valores:

   Nome do alarme

   Insira o nome que você deseja que o Route 53 exiba na coluna Name (Nome) na guia Alarms (Alarmes).

   Descrição do alarme

   (Opcional) Insira uma descrição do alarme. Este valor é exibido no console do CloudWatch.

   Enviar notificação

   Escolha se você deseja que o Route 53 envie uma notificação se o status dessa verificação de integridade acionar um alarme.

   Destino de notificação (somente quando a opção "Enviar notificação" estiver marcada como "Sim")

   Se você quiser que o CloudWatch envie uma notificação para um tópico existente do SNS, escolha o tópico na lista.

   Se você quiser que o CloudWatch envie notificações, exceto para um tópico existente do SNS, faça o seguinte:

   - Se desejar que o CloudWatch envie uma notificação por e-mail, escolha New SNS topic (Novo tópico do SNS) e continue com este procedimento.
   - Se quiser que o CloudWatch envie notificações por outro método, abra uma nova guia do navegador, acesse o console do Amazon SNS e crie o novo tópico. Em seguida, volte para o console do Route 53, escolha o nome do novo tópico na lista Notification target (Destino da notificação) e continue com este procedimento.

   Nome do tópico (somente quando você optar por criar um novo tópico do Amazon SNS)

   Insira um nome para o novo tópico do Amazon SNS.

   Endereços de e-mail do destinatário (somente quando você opta por criar um novo tópico do Amazon SNS)

   Insira o endereço de e-mail para o qual você deseja que o Route 53 envie notificações do SNS quando uma verificação de integridade acionar um alarme.

Destino do alarme

Escolha o valor que você deseja que o Route 53 avalie nesta verificação de integridade:

- Health check status (Status da verificação de integridade): os verificadores de integridade do Route 53 relatam se a verificação está íntegra ou não íntegra
- Health checkers that report the endpoint healthy (%) (Verificadores de integridade que relatam o endpoint como íntegro [%]) (verificações de integridade que monitoram somente um endpoint): a porcentagem dos verificadores de integridade do Route 53 que relatam que o status da verificação de integridade é íntegro
- Number of healthy child health checks (Número de verificações de integridade filhas íntegras) (somente verificações de integridade calculadas): o número de verificações de integridade filhas em uma verificação de integridade calculada que relata se o status da verificação de integridade é íntegro
- TCP connection time (Tempo de conexão TCP) (somente verificações de integridade HTTP e TCP): o tempo em milissegundos usado pelos verificadores de integridade do Route 53 para estabelecer uma conexão TCP com o endpoint
- Time to complete SSL handshake (Tempo para concluir o handshake do SSL) (somente verificações de integridade HTTPS): o tempo em milissegundos usado para os verificadores de integridade do Route 53 concluírem o handshake do SSL/TLS
- Time to first byte (Tempo até o primeiro byte) (somente verificações de integridade HTTP e HTTPS): o tempo em milissegundos usado pelos verificadores de integridade do Route 53 para receber o primeiro byte da resposta a uma solicitação HTTP ou HTTPS

Destino do alarme

Para os destinos de alarme com base em latência (TCP connection time [Tempo de conexão TCP], Time to complete SSL handshake [Tempo até a conclusão do handshake do SSL] e Time to first byte [Tempo até o primeiro byte]), escolha se você deseja que o CloudWatch calcule a latência dos verificadores de integridade do Route 53 em uma região específica ou em todas as regiões (Global).

Se você escolher uma região, o Route 53 medirá a latência somente duas vezes por minuto, e o número de amostras será menor do que se você escolher todas as regiões. É provável que isso resulte em valores mais distantes. Para evitar notificações de alarme falsas, recomendamos que você especifique um número maior de períodos consecutivos cujas verificações de integridade precisam falhar para que o CloudWatch envie as notificações.

Condição de cumprimento

Use as seguintes configurações para determinar quando o CloudWatch deve acionar um alarme.

Destino do alarme	Condição recomendada	Descrição
Status da verificação de integridade	Minimum (Mínimo) < 1	Os verificadores de integridade do Route 53 informam quando o endpoint não é íntegro.
Verificadores de integridade que relatam o endpoint como íntegro (%)	Average (Média) < porcentagem desejada	Verificações de integridade que monitoram somente um endpoint: o Route 53 considera o status de uma verificação de integridade como não íntegro quando menos de 18% dos verificadores de integridade relatam que o status é íntegro. Não escolha Sample Count (Contagem de amostras) para essa métrica, pois o intervalo de contagens de amostra pode ser alterado conforme o Route 53 adiciona mais regiões de verificação de integrida de. Average (Média) sempre representará com precisão a porcentagem de verificad ores que estão indicando o status de uma verificação de integridade.
Número de verificações de integrida de dependentes íntegras	Minimum (Mínimo) < o número desejado de verificações de integridade filhas íntegras	A estatística Mínimo retorna o valor mais conservador e representa o pior cenário.

Destino do alarme	Condição recomendada	Descrição
Tempo de conexão TCP	Média > tempo desejado em milissegundos	Média é um valor mais consistente em comparação com outras estatísticas.
Tempo até a conclusão do handshake do SSL	Média > tempo desejado em milissegundos	Média é um valor mais consistente em comparação com outras estatísticas.
Tempo até o primeiro byte	Média > tempo desejado em milissegundos	Média é um valor mais consistente em comparação com outras estatísticas.

Por pelo menos ***x*** períodos consecutivos de ***y*** minutos/horas/dias

Especifique por quantos períodos consecutivos o valor especificado precisa atender aos critérios para que o Route 53 envie uma notificação. Em seguida, especifique o tamanho do período.

6. Ao escolher Create (Criar), o Amazon SNS envia um e-mail para você com informações sobre o novo tópico do SNS.
7. No e-mail, escolha Confirm subscription. Você precisa confirmar a assinatura para começar a receber as notificações do CloudWatch.

Para visualizar o status de alarme do CloudWatch e editar alarmes do Amazon Route 53 (console)

1. No painel de navegação do console do Route 53, escolha Health Checks (Verificações de integridade).
2. Escolha a linha para qualquer verificação de integridade.
3. No painel de detalhes (depois de x Health Checks Selected (Verificações de integridade selecionadas)), selecione o ícone de seta para a direita ( ).

A lista CloudWatch Alarms (Alarmes do CloudWatch) contém todos os alarmes do Route 53 que você criou usando a conta atual da AWS.

A coluna Estado mostra o status atual de cada alarme:

OK

O CloudWatch acumulou estatísticas suficientes das verificações de integridade do Route 53 para determinar se o endpoint não atende ao limite de alarme.

DADOS INSUFICIENTES

O CloudWatch não acumulou estatísticas suficientes para determinar se o endpoint atende ou não ao limite de alarme. Este é o estado inicial de um novo alarme. O estado do alarme também mudará para INSUFFICIENT DATA (DADOS INSUFICIENTES) se as métricas do CloudWatch ficarem indisponíveis ou se você excluir a verificação de integridade sem excluir o alarme associado.

ALARME

O CloudWatch acumulou estatísticas suficientes das verificações de integridade do Route 53 para determinar que o endpoint atende ao limite de alarme e enviar uma notificação ao endereço de e-mail especificado.

4. Para visualizar ou editar as configurações de um alarme, escolha o nome do alarme.
5. Para visualizar um alarme no console do CloudWatch, com informações mais detalhadas sobre o alarme (por exemplo, um histórico de atualizações do alarme e alterações de status), escolha a opção View (Visualizar) na coluna More Options (Mais opções) do alarme.
6. Para visualizar todos os alarmes do CloudWatch que você criou usando a conta atual da AWS, incluindo alarmes de outros serviços da AWS, escolha a opção View All CloudWatch Alarms (Visualizar todos os alarmes do CloudWatch).
7. Para visualizar todas as métricas disponíveis do CloudWatch, incluindo métricas que não estão sendo usadas no momento pela conta atual da AWS, escolha a opção View All CloudWatch Metrics (Visualizar todas as métricas do CloudWatch).

Para visualizar as métricas do Route 53 usando o console do Amazon CloudWatch

1. Faça login no AWS Management Console e abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. Altere a região atual para Leste dos EUA (Norte da Virgínia). As métricas do Route 53 não ficarão disponíveis, se você selecionar qualquer outra região como a atual.
3. No painel de navegação, escolha Metrics (Métricas).

4. Na guia Todas as métricas, escolha Route 53.
5. Escolha Métricas de verificação de integridade.

Configurar failover de DNS

Quando houver mais de um recurso executando a mesma função, (por exemplo, mais de um servidor HTTP ou servidor de e-mail), você poderá configurar o Amazon Route 53 para verificar a integridade dos seus recursos e responder às consultas de DNS usando somente os recursos íntegros. Por exemplo, suponhamos que seu site, example.com, esteja hospedado em seis servidores distribuídos por três datacenters ao redor do mundo (dois servidores em cada). Você pode configurar o Route 53 para verificar a integridade desses servidores e responder às consultas de DNS de example.com usando somente os servidores atualmente considerados como íntegros.

O Route 53 pode verificar a integridade dos seus recursos em configurações simples e complexas:

- Em configurações simples, você cria um grupo de registros com o mesmo nome e tipo, por exemplo, um grupo de registros ponderados com um tipo A para example.com. Em seguida, configure o Route 53 para verificar a integridade dos recursos correspondentes. O Route 53 responde às consultas de DNS com base na integridade dos seus recursos. Para obter mais informações, consulte Como as verificações de integridade funcionam com as configurações simples do Amazon Route 53.
- Em configurações mais complexas, você cria uma árvore de registros que roteia o tráfego com base em vários critérios. Por exemplo, se a latência para seus usuários for seu critério mais importante, você poderá usar registros com alias de latência para rotear o tráfego para a região que fornece a melhor latência. Os registros com alias de latência podem ter registros ponderados em cada região como o destino do alias. Os registros ponderados podem rotear o tráfego para instâncias do EC2 com base no tipo de instância. Como com uma configuração simples, você pode definir o Route 53 para encaminhar o tráfego com base na integridade dos seus recursos. Para obter mais informações, consulte Como as verificações de integridade funcionam com as configurações complexas do Amazon Route 53.

Tópicos

- Como as verificações de integridade funcionam com as configurações complexas do Amazon Route 53
- Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada
- Failover ativo/ativo e ativo-passivo
- Configurar failover em uma zona hospedada privada
- Como o Amazon Route 53 evita problemas de failover

Lista de tarefas para configurar o failover de DNS

Para usar o Route 53 para configurar o failover de DNS, faça o seguinte:

1. Desenhe um diagrama de árvore completo de sua configuração e indique o tipo de registro que você está criando (alias ponderado, failover, latência etc.) para cada nó. No topo da árvore, coloque os registros do nome de domínio (como example.com) que seus usuários usarão para acessar seu site ou aplicativo web.

   Os tipos de registros exibidos no seu diagrama de árvore dependem da complexidade da configuração:

   - Em uma configuração simples, seu diagrama não incluirá nenhum registro com alias ou, então, os registros com alias encaminharão o tráfego diretamente para um recurso (como um balanceador de carga do ELB), em vez de encaminhar para outro registro do Route 53. Para obter mais informações, consulte Como as verificações de integridade funcionam com as configurações simples do Amazon Route 53.
   - Em uma configuração complexa, o diagrama incluirá uma combinação de registros de alias (como alias ponderado e alias de failover) e registros não alias em uma árvore de vários níveis, como os exemplos no tópico Como as verificações de integridade funcionam com as configurações complexas do Amazon Route 53.

   > **Note**
   >
   > Para criar de maneira rápida e fácil registros para configurações de roteamento complexo e associar os registros a verificações de integridade, você pode usar o editor visual de fluxo de tráfego e salvar a configuração como uma política de tráfego. Em seguida, é possível associar a política de tráfego a um ou mais nomes de domínio (como example.com) ou nomes de subdomínio (como www.example.com), na mesma ou em várias zonas hospedadas. Além disso, você poderá reverter as atualizações se

a nova configuração não estiver sendo executada conforme o esperado. Para obter mais informações, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS.

Para obter mais informações, consulte a documentação a seguir:

- Escolher uma política de roteamento
- Escolher entre registros de alias e não alias

2. Crie verificações de integridade para os recursos para os quais você não pode criar registros com alias, como servidores do Amazon EC2 e servidores de e-mail em execução no seu datacenter. Você associará essas verificações de integridade aos seus registros não alias.

   Para obter mais informações, consulte Criar, atualizar e excluir verificações de integridade.

3. Se necessário, configure as regras do roteador e do firewall para que o Route 53 consiga enviar solicitações regulares aos endpoints que você especificou nas suas verificações de integridade. Para obter mais informações, consulte Como configurar regras de roteador e firewall para as verificações de integridade do Amazon Route 53 .

4. Crie todos os registros não alias no seu diagrama e associe as verificações de integridade que criou na etapa 2 aos registros aplicáveis.

   Se você estiver configurando o failover de DNS em uma configuração que não inclui nenhum registro com alias, ignore as tarefas restantes.

5. Crie os registros com alias que encaminham o tráfego para recursos da AWS, como balanceadores de carga do ELB e distribuições do CloudFront. Se quiser que o Route 53 teste outra ramificação da árvore quando um recurso não estiver íntegro, defina o valor de Evaluate Target Health (Avaliar integridade do destino) como Yes (Sim) para cada um de seus registros com alias. (Evaluate Target Health [Avaliar integridade do destino] não é suportado por alguns recursos da AWS.)

6. Começando na parte inferior do diagrama de árvore que você criou na etapa 1, crie os registros com alias que encaminham o tráfego para os registros criados nas etapas 4 e 5. Para que o Route 53 tente outra ramificação da árvore quando nenhum dos registros sem alias estiver íntegro em uma ramificação de sua árvore, defina o valor de Evaluate Target Health (Avaliar integridade do destino) como Yes (Sim) para cada um de seus registros com alias.

   Lembre-se de que você não pode criar um registro com alias que encaminha o tráfego para outro registro até que tenha criado o outro registro.

Como as verificações de integridade funcionam com as configurações simples do Amazon Route 53

Quando há dois ou mais recursos que executam a mesma função, como dois ou mais servidores da Web para example.com, você pode usar os seguintes recursos de verificação de integridade para encaminhar o tráfego somente para os recursos íntegros:

Verifique a integridade de instâncias do EC2 e de outros recursos (registros que não são de alias)

Se você estiver roteando tráfego a recursos para os quais não é possível criar registros com alias, como instâncias do EC2, crie um registro e uma verificação de integridade para cada recurso. Em seguida, associe cada verificação de integridade ao registro aplicável. As verificações de integridade verificam regularmente a integridade dos recursos correspondentes, e o Route 53 encaminha o tráfego apenas para os recursos que relatam as verificações de integridade como íntegras.

Avaliar a integridade de um recurso da AWS (registros com alias)

Se estiver usando registros do alias para encaminhar o tráfego para recursos selecionados da AWS, como balanceadores de carga do ELB, você poderá configurar o Route 53 para avaliar a integridade do recurso e encaminhar o tráfego apenas para recursos íntegros. Quando você configura um registro com alias para avaliar a integridade de um recurso, não é necessário criar uma verificação de integridade para ele.

Aqui está uma visão geral de como configurar o Route 53 para verificar a integridade dos recursos em configurações simples:

1. Você identifica os recursos que você deseja que o Route 53 monitore. Por exemplo, convém monitorar todos os servidores HTTP que respondem às solicitações de example.com.
2. Você cria verificações de integridade para recursos para os quais não é possível criar registros com alias, como instâncias do EC2 ou servidores no seu próprio datacenter. Você especifica como enviar solicitações de verificação de integridade para o recurso: qual protocolo usar (HTTP, HTTPS ou TCP), qual endereço IP e porta usar e, para verificações de integridade HTTP/HTTPS, um nome de domínio e caminho.

> **Note**
>
> Se você estiver usando algum recurso para o qual possa criar registros com alias, como os load balancers do ELB, não crie verificações de integridade para esses recursos.

Uma configuração comum é criar uma verificação de integridade para cada recurso e usar o mesmo endereço IP para o endpoint de verificação de integridade e para o recurso. A verificação de integridade envia solicitações para o endereço IP especificado.

> **Note**
>
> O Route 53 não pode verificar a integridade de recursos que possuem um endereço IP nos intervalos locais, privados, não encaminháveis ou multicast. Para mais informações sobre os endereços IP para os quais não é possível criar verificações de integridade, consulte RFC 5735, Endereços IPv4 de uso especial e RFC 6598, Prefixo IPv4 reservado por IANA para espaço de endereço compartilhado.

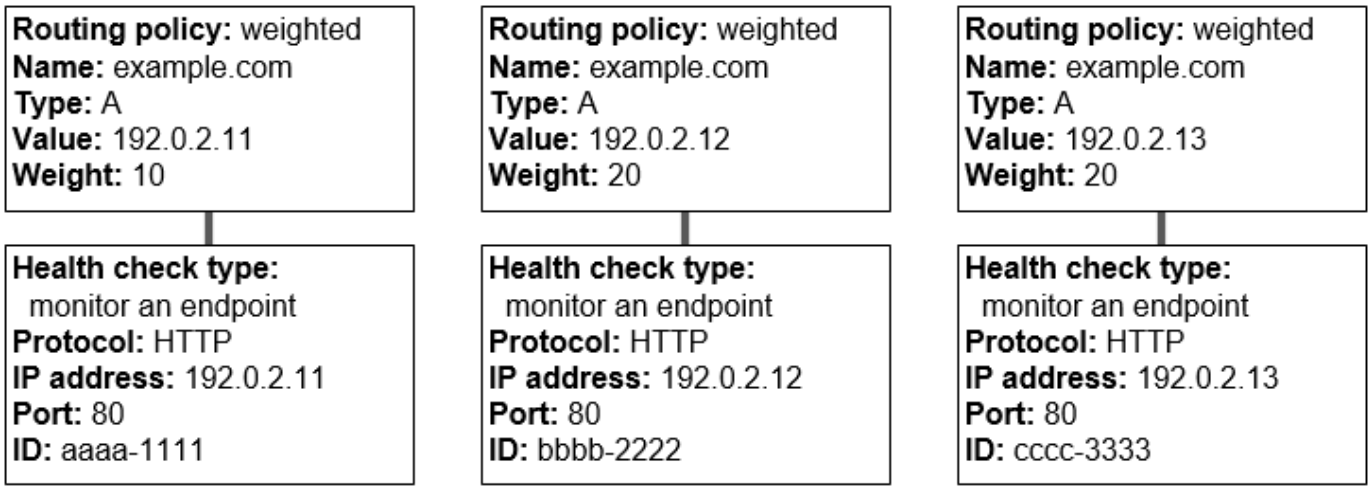
Para obter mais informações sobre como criar verificações de integridade, consulte Criar, atualizar e excluir verificações de integridade.

3. Talvez seja necessário configurar as regras do roteador e do firewall para que o Route 53 consiga enviar solicitações regulares aos endpoints que você especificou nas suas verificações de integridade. Para obter mais informações, consulte Como configurar regras de roteador e firewall para as verificações de integridade do Amazon Route 53 .
4. Você cria um grupo de registros para seus recursos, por exemplo, um grupo de registros ponderados. Você pode combinar registros com alias e sem alias, mas todos eles devem ter o mesmo valor para Name, Type e Routing Policy.

   A maneira de configurar o Route 53 para verificar a integridade dos seus recursos depende se você está criando registros com alias ou sem alias:

   - Alias records (Registros com alias): especifique Yes (Sim) para Evaluate Target Health (Avaliar integridade do destino).
   - Non-alias records (Registros sem alias): associe as verificações de integridade que você criou na etapa 2 com os registros correspondentes.

Quando terminar, sua configuração será semelhante ao diagrama a seguir, que inclui apenas os registros sem alias.



Para obter mais informações sobre como criar registros usando o console do Route 53, consulte Criar registros usando o console do Amazon Route 53.

5. Se você criou verificações de integridade, o Route 53 enviará solicitações periódicas ao endpoint para cada verificação de integridade. Ele não executará a verificação de integridade quando receber uma consulta de DNS. Com base nas respostas, o Route 53 decide se os endpoints são íntegros e usa essa informação para determinar como responder às consultas. Para obter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

   O Route 53 não verifica a integridade do recurso especificado no registro, como o endereço IP especificado em um registro A para example.com. Quando você associa uma verificação de integridade a um registro, o Route 53 inicia a verificação de integridade do endpoint especificado na verificação de integridade. Você também pode configurar o Route 53 para monitorar a integridade de outras verificações de integridade ou os fluxos de dados dos alarmes do CloudWatch. Para obter mais informações, consulte Tipos de verificações de integridade do Amazon Route 53.

Veja a seguir o que acontece quando o Route 53 recebe uma consulta para example.com:

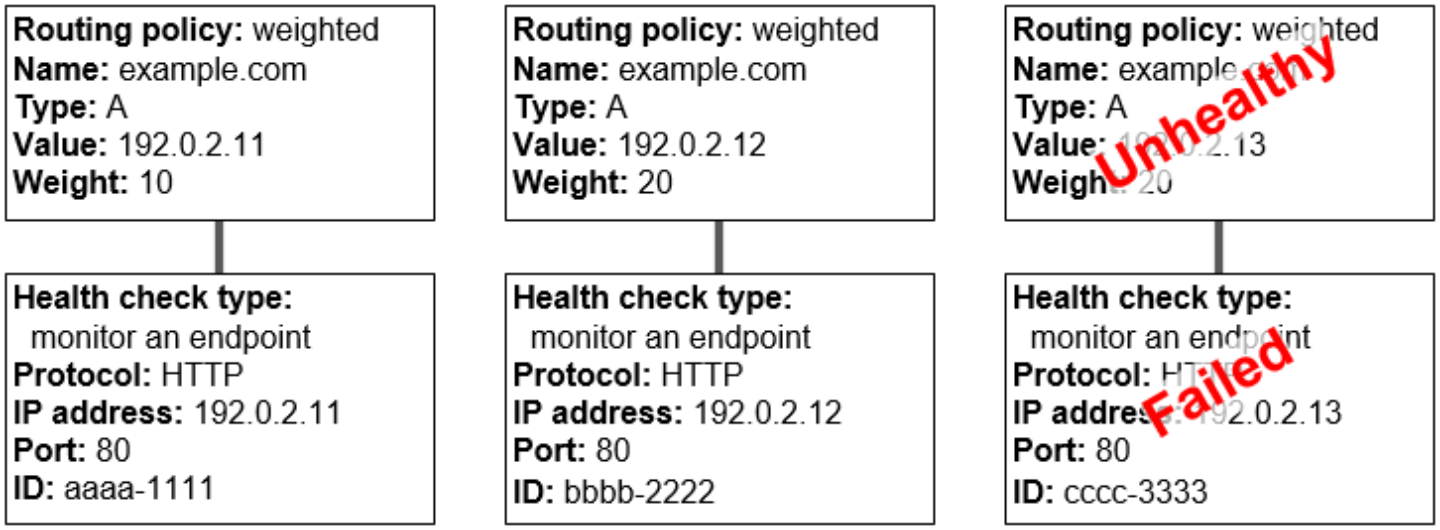
1. O Route 53 escolhe um registro com base na política de roteamento. Nesse caso, ele escolhe um registro com base no peso.

2. Ele determina a integridade atual do registro selecionado verificando o status da verificação de integridade desse registro.
3. Se o registro selecionado não for íntegro, o Route 53 escolherá um registro diferente. Dessa vez, o registro não íntegro não é considerado.

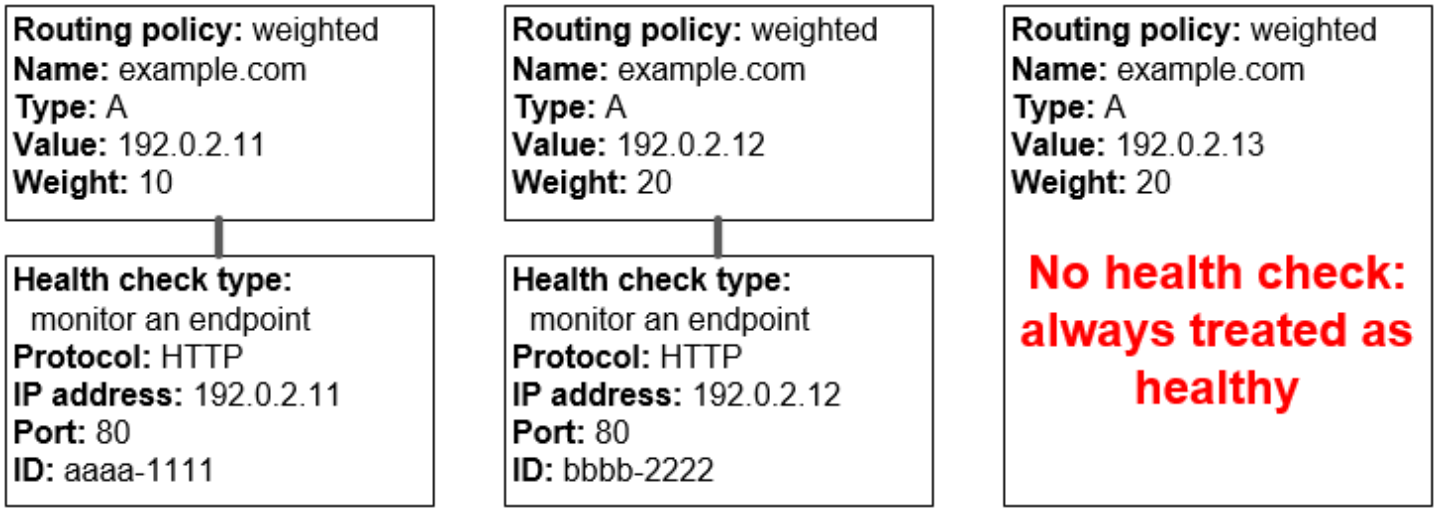
   Para obter mais informações, consulte Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada.
4. Quando o Route 53 encontra um registro íntegro, ele responde à consulta com o valor aplicável, como o endereço IP em um registro A.

O exemplo a seguir mostra um grupo de registros ponderados em que o terceiro registro não está íntegro. Inicialmente, o Route 53 seleciona um registro com base nos pesos de todos os três registros. Se ele selecionar o registro não íntegro na primeira vez, o Route 53 selecionará outro registro, mas, dessa vez, omitirá o peso do terceiro registro do cálculo:

- Inicialmente, quando o Route 53 seleciona entre todos os três registros, ele responde às solicitações usando o primeiro registro cerca de 20% do tempo, 10/(10 + 20 + 20).
- Quando o Route 53 determina que o terceiro registro não está íntegro, ele responde às solicitações usando o primeiro registro cerca de 33% do tempo, 10/(10 + 20).



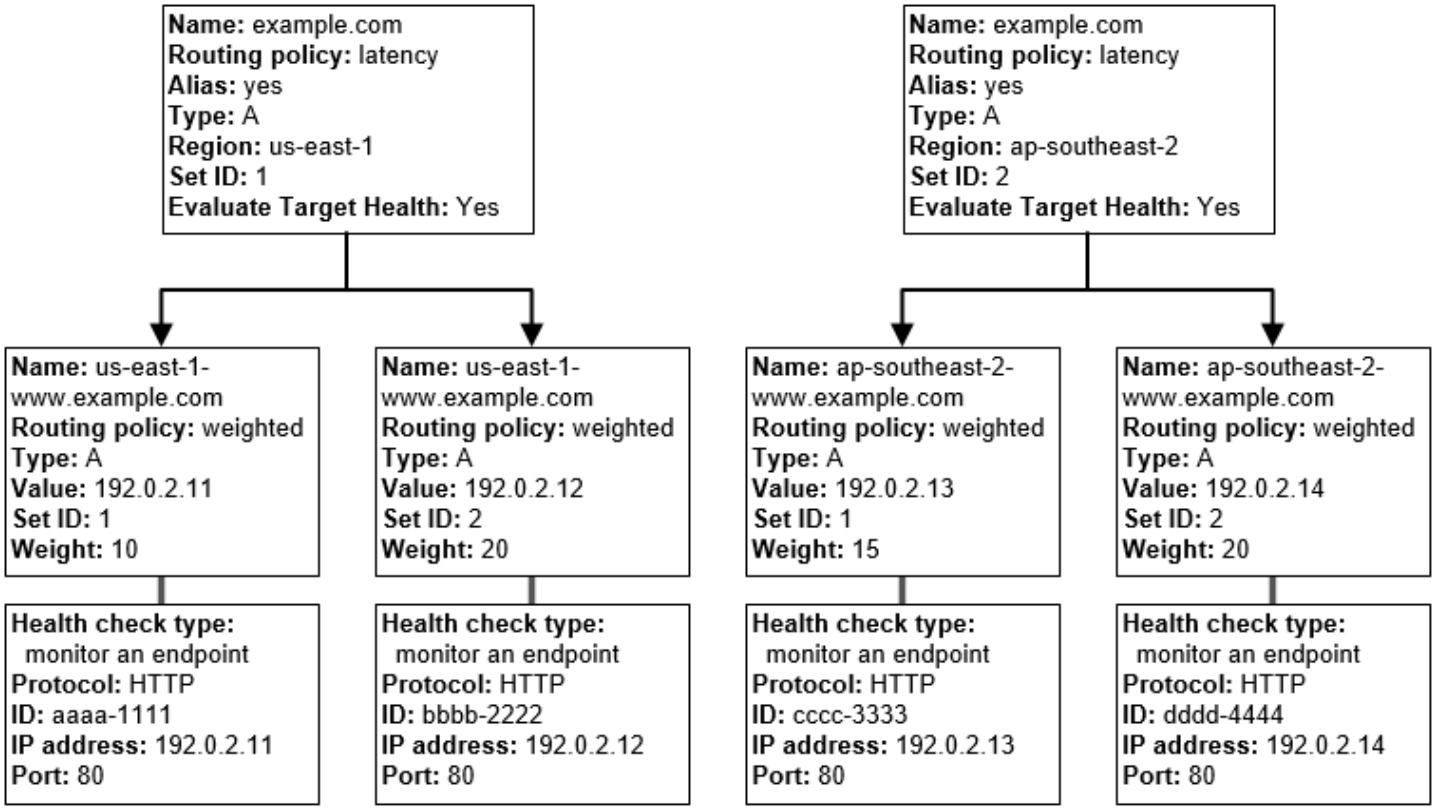
Se você omitir uma verificação de integridade de um ou mais registros em um grupo de registros, o Route 53 não poderá determinar a integridade do recurso correspondente. O Route 53 os tratará como registros íntegros.



Como as verificações de integridade funcionam com as configurações complexas do Amazon Route 53

A verificação da integridade dos recursos em configurações complexas funciona da mesma forma que nas configurações simples. No entanto, em configurações complexas, você usa uma combinação de registros com alias (como alias ponderados e alias de failover) e registros de não alias para construir uma árvore de decisão que fornece maior controle sobre como o Route 53 responde às solicitações.

Por exemplo, você pode usar registros de alias de latência para selecionar uma região próxima a um usuário e usar registros ponderados para dois ou mais recursos em cada região para se proteger contra a falha de um único endpoint ou de uma zona de disponibilidade. O diagrama a seguir mostra essa configuração.



Veja como o Amazon EC2 e o Route 53 são configurados. Vamos começar na parte inferior da árvore porque essa é a ordem em que você criará registros:

- Você tem duas instâncias do EC2 em cada uma das suas regiões, us-east-1 e ap-southeast-2. Você quer que o Route 53 roteie o tráfego para suas instâncias do EC2 levando em consideração o estado de integridade delas. Portanto, crie uma verificação de integridade para cada instância. Você configura cada verificação de integridade para enviar solicitações de verificação de integridade à instância correspondente no endereço IP elástico da instância.

  O Route 53 é um serviço global. Portanto, você não especifica a região em que quer criar verificações de integridade.

- Convém rotear o tráfego para as duas instâncias em cada região com base no tipo de instância, de modo que você possa criar um registro ponderado para cada instância e atribuir um peso a cada registro. (Você pode alterar o peso posteriormente para rotear mais ou menos tráfego para uma instância.) Você também associa a verificação de integridade aplicável a cada instância.

  Quando você cria os registros, você usa nomes, como us-east-1-www.exemplo.com. e ap-southeast-2-www.exemplo.com. Você esperará até chegar ao topo da árvore para fornecer aos

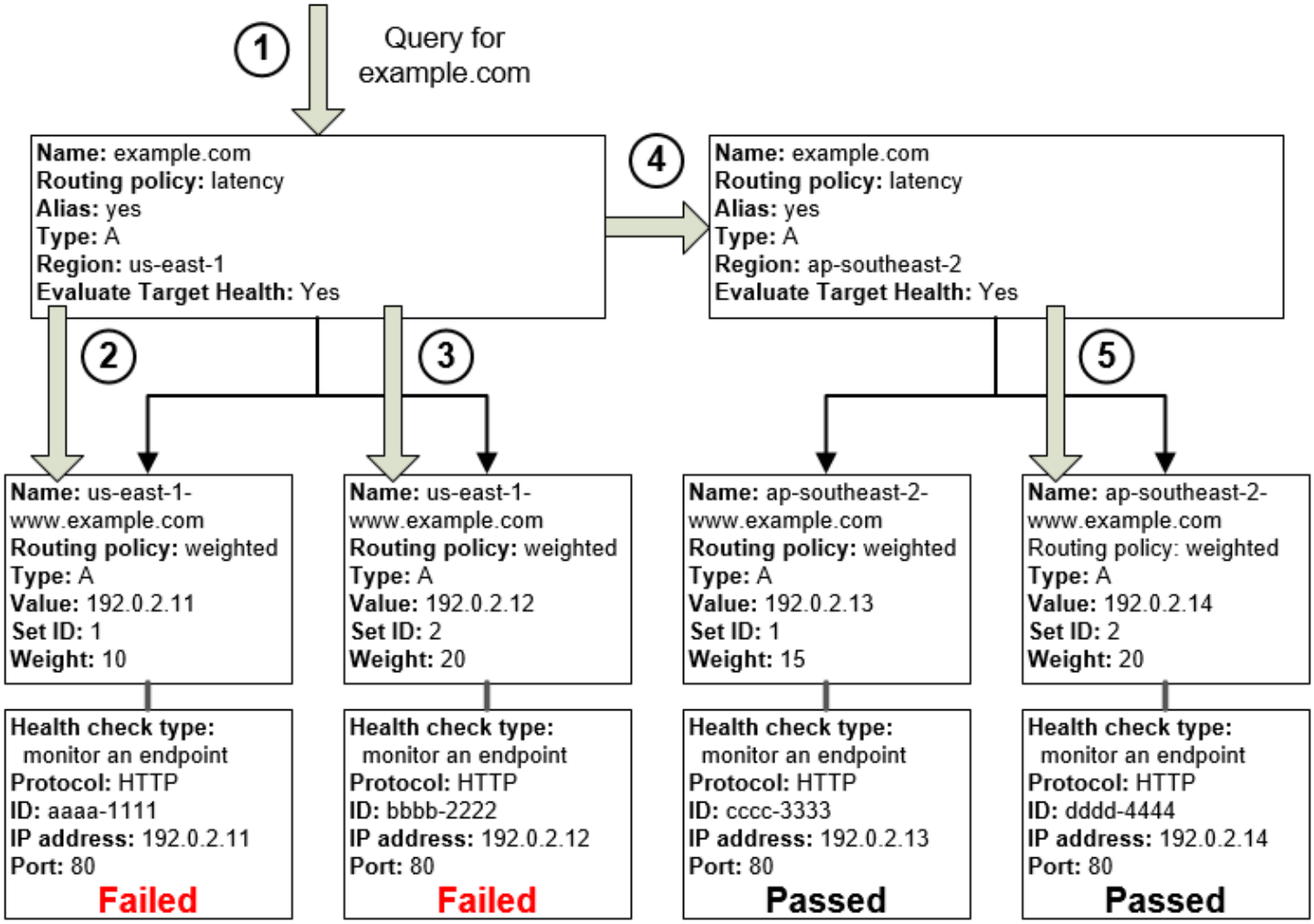
registros os nomes que seus usuários usarão para acessar seu site ou aplicativo web, como example.com.

- Convém direcionar o tráfego para a região que fornece a menor latência para seus usuários, para que você possa escolher a política de roteamento da latência para os registros no topo da árvore.

  Convém direcionar o tráfego para os registros em cada região, e não diretamente para os recursos em cada região (os registros ponderados já fazem isso). Como resultado, você cria registros com alias de latência.

  Ao criar os registros com alias, você fornece o nome que deseja que seus usuários usem para acessar seu site ou aplicativo web, como example.com. Os registros com alias roteiam o tráfego de example.com para os registros de us-east-1-www.example.com e ap-southeast-2-www.example.com.

  Para os dois registros de alias de latência, defina o valor de Evaluate Target Health como Yes. Isso faz com que o Route 53 determine se há algum recurso íntegro em uma região antes de tentar encaminhar o tráfego para lá. Caso contrário, o Route 53 escolherá um recurso íntegro na outra região.



O diagrama anterior ilustra a seguinte sequência de eventos:

1. O Route 53 recebe uma consulta para example.com. Com base na latência do usuário que faz a solicitação, o Route 53 seleciona o registro de alias de latência para a região us-east-1.
2. O Route 53 seleciona um registro ponderado com base no peso. Evaluate Target Health (Avaliar integridade do destino) é Yes (Sim) para o registro com alias de latência, portanto, o Route 53 verifica a integridade do registro ponderado selecionado.
3. A verificação de integridade falhou, portanto, o Route 53 escolhe outro registro ponderado com base no peso e verifica sua integridade. Este registro também não está íntegro.
4. O Route 53 retorna à ramificação da árvore, procura o registro de alias de latência com a segunda melhor latência, e escolhe o registro para ap-southeast-2.
5. O Route 53 seleciona novamente um registro com base no peso e, em seguida, verifica a integridade do recurso selecionado. O recurso é íntegro. Portanto, o Route 53 retornará o valor aplicável em resposta à consulta.

Tópicos

O que acontece quando você associa uma verificação de integridade a um registro de alias?

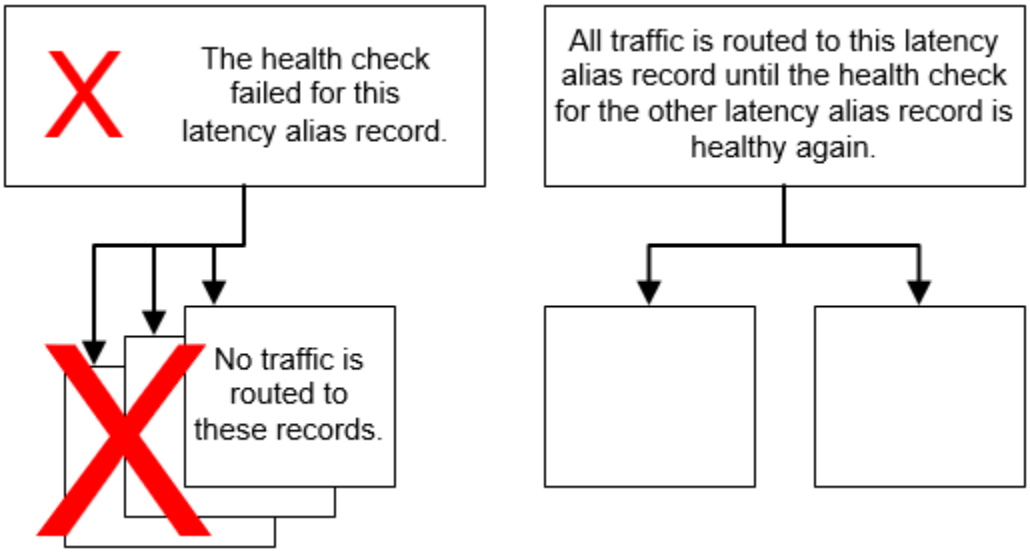
Você pode associar uma verificação de integridade a um registro de alias em vez de ou além de configurar o valor de Evaluate Target Health como Yes. No entanto, geralmente é mais útil que o Route 53 responda às consultas com base na integridade dos recursos subjacentes, os servidores HTTP, os servidores de banco de dados e outros recursos aos quais seus registros de alias se referem. Por exemplo, suponha a seguinte configuração:

- Você atribui uma verificação de integridade a um registro de alias de latência no qual o destino do alias é um grupo de registros ponderados.
- Você define o valor de Evaluate Target Health como Yes para o registro de alias de latência.

Nessa configuração, os seguintes itens precisam ser verdadeiros para que o Route 53 retorne o valor aplicável para um registro ponderado:

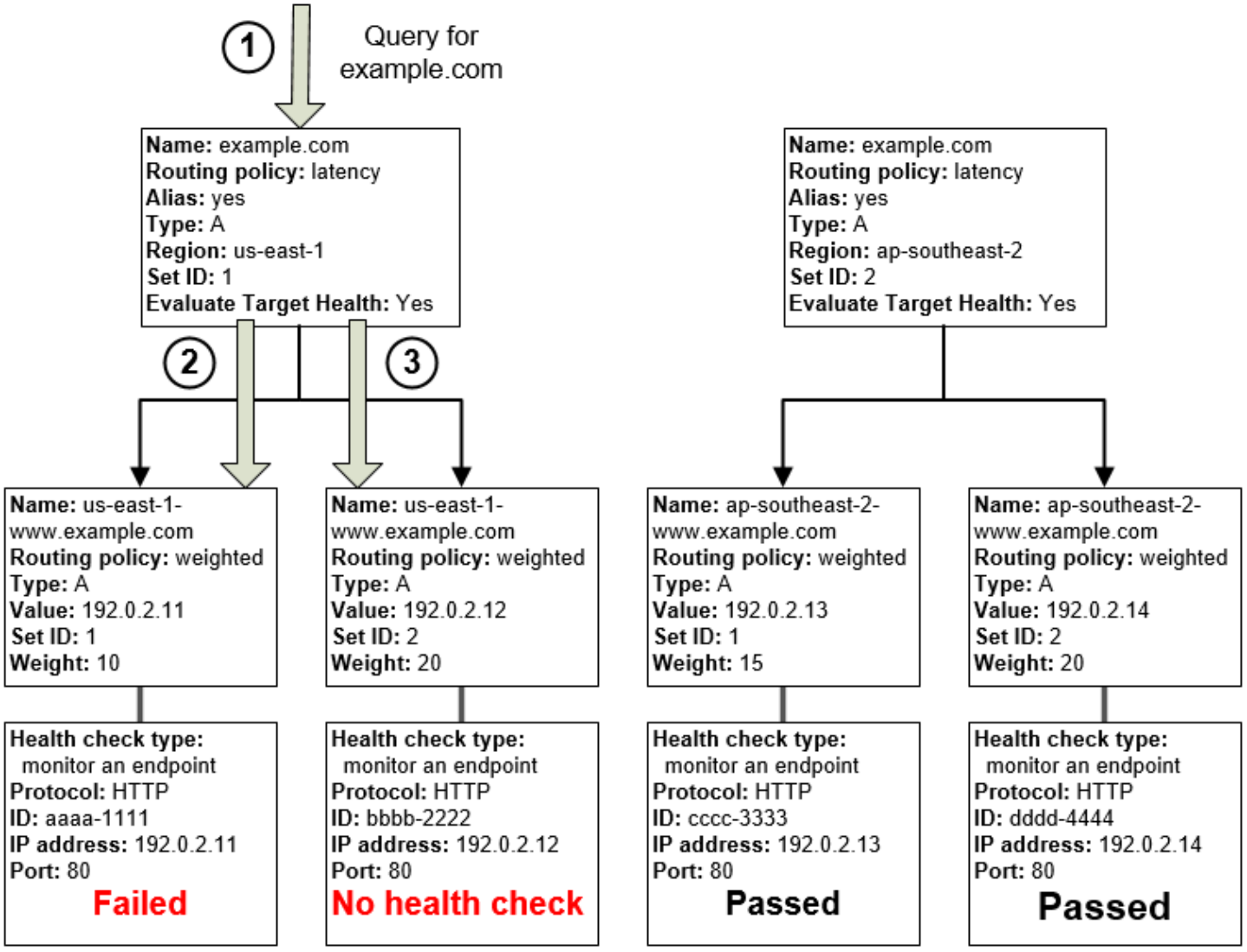
- A verificação de integridade associada ao registro de alias de latência deve ser aprovada.
- Pelo menos um registro ponderado precisa ser considerado íntegro, seja porque ele está associado a uma verificação de integridade aprovada ou porque não está associado a uma verificação de integridade. No último caso, o Route 53 sempre considera o registro ponderado como íntegro.

Na ilustração a seguir, a verificação de integridade do registro com alias de latência no canto superior esquerdo apresentou falha. Como resultado, o Route 53 deixará de responder às consultas usando qualquer um dos registros ponderados aos quais o registro com alias de latência se refere, mesmo que todos estejam em bom estado. O Route 53 só começará a considerar esses registros ponderados novamente quando a verificação de integridade do registro com alias de latência voltar ao estado íntegro. (Para exceções, consulte Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada.)



O que acontece quando você omite verificações de integridade?

Em uma configuração complexa, é importante associar as verificações de integridade a todos os registros sem alias. No exemplo a seguir, está faltando uma verificação de integridade em um dos registros ponderados na região us-east-1.



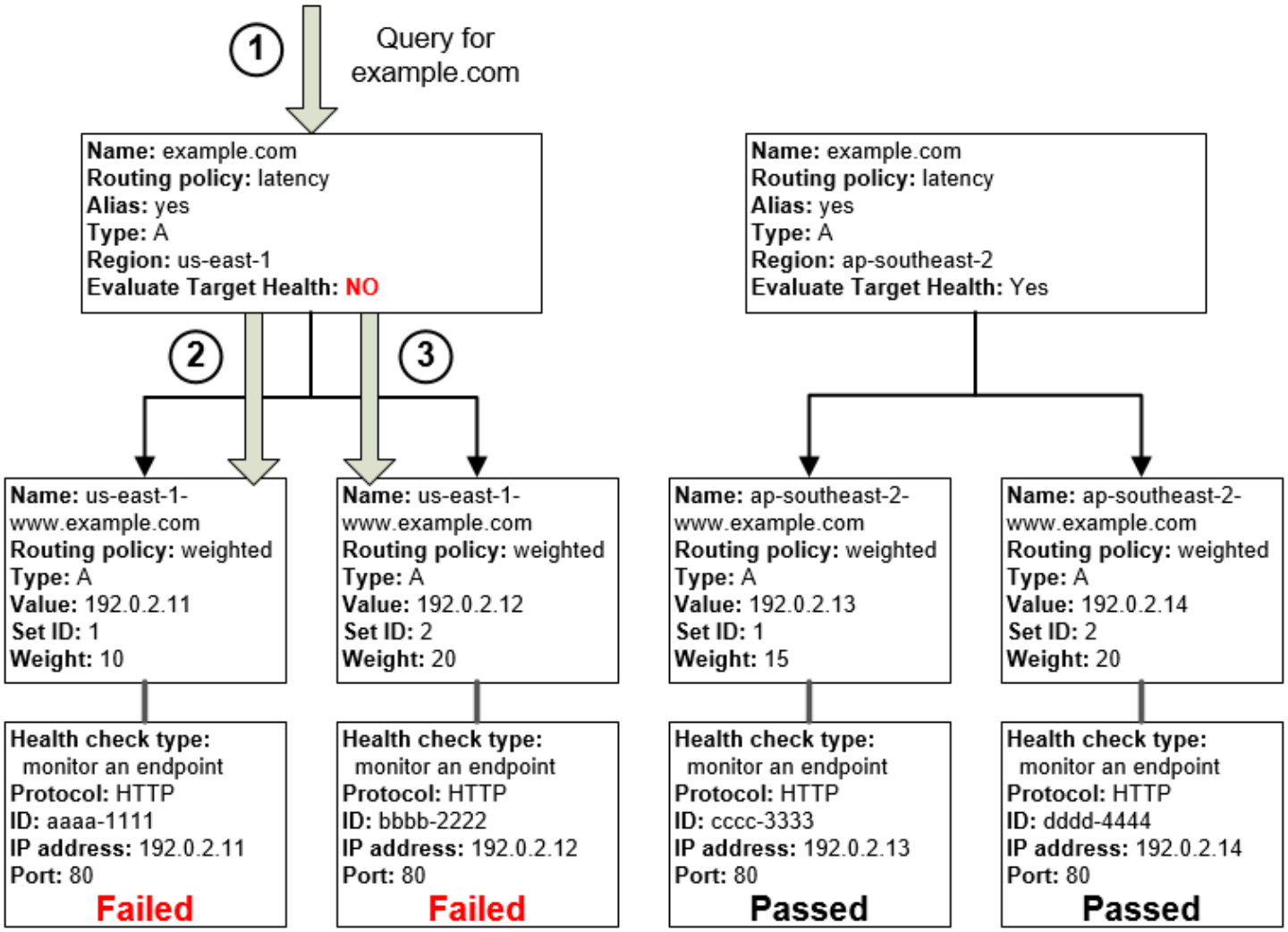
Veja o que acontece quando você omite uma verificação de integridade em registro não alias nessa configuração:

1. O Route 53 recebe uma consulta para example.com. Com base na latência do usuário que faz a solicitação, o Route 53 seleciona o registro de alias de latência para a região us-east-1.
2. O Route 53 procura o destino do alias para o registro de alias de latência e verifica o status das verificações de integridade correspondentes. A verificação de integridade de um registro ponderado falhou, portanto esse registro não é considerado.
3. O outro registro ponderado no destino do alias para a região us-east-1 não possui verificação de integridade. O recurso correspondente pode ou não ser íntegro, mas sem uma verificação de integridade, o Route 53 não tem como saber. O Route 53 presume que o recurso seja íntegro e retorna o valor aplicável em resposta à consulta.

O que acontece quando você define avaliar a integridade do alvo como Não?

Em geral, você deve definir Evaluate Target Health como Yes para todos os registros com alias em uma árvore. Se você definir Evaluate Target Health (Avaliar integridade do destino) como No (Não), o Route 53 continuará encaminhando o tráfego para os registros aos quais um registro com alias se refere, mesmo que as verificações de integridade deles apresentem falha.

Neste exemplo, todos os registros ponderados têm verificações de integridade associadas, mas Evaluate Target Health está definido como No para o registro com alias de latência da região us-east-1:



Veja a seguir o que acontece quando você define Evaluate Target Health como No em um registro de alias nessa configuração:

1. O Route 53 recebe uma consulta para example.com. Com base na latência do usuário que faz a solicitação, o Route 53 seleciona o registro de alias de latência para a região us-east-1.

2. O Route 53 determina qual é o destino do alias para o registro de alias de latência e confere as verificações de integridade correspondentes. Ambas falham.
3. Como o valor de Evaluate Target Health (Avaliar integridade do destino) é No (Não) para o registro com alias de latência da região us-east-1, o Route 53 precisa escolher um registro nessa ramificação, em vez de sair dela e procurar um registro íntegro na região ap-southeast-2.

Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada

Se você configurar a verificação de integridade para todos os registros em um grupo de registros com o mesmo nome, o mesmo tipo (como A ou AAAA) e a mesma política de roteamento (como ponderada ou failover), o Route 53 responderá às consultas de DNS escolhendo um registro íntegro e retornando o valor aplicável desse registro.

Por exemplo, suponha que você crie três registros A ponderados e atribua verificações de integridade a todos eles. Se a verificação de integridade de um dos registros não for íntegra, o Route 53 responderá às consultas de DNS com os endereços IP em um dos outros dois registros.

Veja como o Route 53 escolhe um registro íntegro:

1. Inicialmente, o Route 53 escolhe um registro com base na política de roteamento e nos valores que você especifica para cada registro. Por exemplo, para registros ponderados, o Route 53 escolhe um registro baseado no peso que você especifica para cada registro.
2. O Route 53 determina se o registro é íntegro:
   - Non-alias record with an associated health check (Registro sem alias com uma verificação de integridade associada): se você tiver associado uma verificação de integridade a um registro sem alias, o Route 53 verificará o status atual da verificação de integridade.

     O Route 53 verifica periodicamente a integridade do endpoint especificado em uma verificação de integridade. Ele não executa a verificação de integridade quando recebe a consulta de DNS.

     Você pode associar verificações de integridade a registros com alias, mas recomendamos que associe as verificações de integridade apenas aos registros sem alias. Para obter mais informações, consulte O que acontece quando você associa uma verificação de integridade a um registro de alias?.
   - Alias record with Evaluate Target Health set to Yes (Registro com alias com Avaliar integridade do destino definida como Sim): o Route 53 verifica o status da integridade do recurso ao qual

o registro com alias faz referência, por exemplo, um balanceador de carga do ELB ou outro registro na mesma zona hospedada.

3. Se o registro estiver íntegro, o Route 53 responderá à consulta com o valor aplicável, como um endereço IP.

   Se o registro não for íntegro, o Route 53 escolherá outro registro usando os mesmos critérios e repetirá o processo até encontrar um registro íntegro.

O Route 53 usa os seguintes critérios ao escolher um registro:

Registros sem uma verificação de integridade são sempre íntegros

Se um registro em um grupo de registros com o mesmo nome e tipo não tiver uma verificação de integridade associada, o Route 53 sempre o considerará íntegro e o incluirá entre as possíveis respostas a uma consulta.

Se nenhum registro for íntegro, todos os registros serão íntegros

Se nenhum dos registros em um grupo de registros estiver íntegro, o Route 53 precisará retornar algo em resposta às consultas DNS, mas não terá base para escolher um registro em de vez de outro. Nessa circunstância, o Route 53 considerará todos os registros no grupo como íntegros e selecionará um deles com base na política de roteamento e nos valores que você especifica para cada registro.

Registros ponderados com um peso de 0

Se você adicionar verificações de integridade a todos os registros em um grupo de registros ponderados, mas atribuir pesos diferentes de zero a alguns registros e pesos iguais a zero a outros, as verificações de integridade funcionarão da mesma maneira que todos os registros com pesos diferentes de zero com as seguintes exceções:

- Inicialmente, o Route 53 considera somente os registros ponderados com valores diferentes de zero, se houver.
- Se nenhum dos registros com ponderação maior que zero estiver íntegro, o Route 53 considerará os registros com ponderação igual a zero.

Como o Route 53 considera os registros com peso zero em algumas circunstâncias, é importante garantir que o destino de peso zero também tenha uma resposta viável para uma consulta ao DNS.

Para obter mais informações sobre registros ponderados, consulte Verificações de integridade e roteamento ponderado.

Registros de alias

Você também pode configurar a verificação de integridade para registros com alias, definindo Evaluate Target Health como Yes para cada registro com alias. Isso faz com que o Route 53 avalie a integridade do recurso para o qual o registro direciona o tráfego, por exemplo, um balanceador de carga do ELB ou outro registro na mesma zona hospedada.

Por exemplo, suponhamos que o destino de um registro com alias ponderado seja um grupo de registros ponderados, todos com pesos diferentes de zero:

- Desde que pelo menos um dos registros ponderados esteja íntegro, o Route 53 considerará o registro com alias como íntegro.
- Se nenhum registro ponderado estiver íntegro, o Route 53 não considerará o registro com alias como íntegro.
- O Route 53 deixará de considerar os registros nessa ramificação da árvore até que pelo menos um registro ponderado torne-se íntegro novamente.

Para obter mais informações, consulte Como as verificações de integridade funcionam com as configurações complexas do Amazon Route 53.

Registros de failover

Os registros de failover geralmente funcionam da mesma maneira que outros tipos de roteamento. Você cria verificações de integridade, as associa aos registros de sem alias e define Evaluate Target Health como Yes para registros com alias. Observe o seguinte:

- Os registros primário e secundário podem ser um registro sem alias ou um registro com alias.
- Se você associar verificações de integridade aos registros de failover primário e secundário, o Route 53 responderá às solicitações da seguinte maneira:
  - Se o Route 53 considerar o registro primário íntegro (se o endpoint da verificação de integridade estiver íntegro), o Route 53 retornará somente o registro primário em resposta a uma consulta de DNS.
  - Se o Route 53 considerar o registro primário como não íntegro, e o registro secundário como íntegro, o Route 53 retornará o registro secundário em vez do primário.
  - Se o Route 53 considerar os registros primário e secundário como não íntegros, o Route 53 retornará o registro primário.

- Ao configurar o registro secundário, a adição de uma verificação de integridade é opcional. Se você omitir a verificação de integridade do registro secundário, e se o endpoint da verificação de integridade do registro primário não estiver íntegro, o Route 53 sempre responderá às consultas de DNS usando o registro secundário. Isso acontece mesmo que o registro secundário não seja íntegro.

Para obter mais informações, consulte os tópicos a seguir:

- Configurar failover ativo/passivo com um recurso principal e um recurso secundário
- Configurar failover ativo/passivo com vários recursos principais e secundários

Failover ativo/ativo e ativo-passivo

Você pode usar a verificação de integridade do Route 53 para definir configurações de failover ativo-ativo e ativo-passivo. Você configura o failover ativo-ativo usando qualquer política de roteamento (ou combinação de políticas de roteamento) diferente de failover, e configura o failover ativo-passivo usando a política de roteamento de failover.

Tópicos

- Failover ativo/ativo
- Failover ativo/passivo

Failover ativo/ativo

Use essa configuração de failover quando você quiser que todos os seus recursos permaneçam disponíveis na maioria do tempo. Quando um recurso se torna indisponível, o Route 53 detecta que ele não é íntegro e deixa de incluí-lo ao responder às consultas.

No failover ativo-ativo, todos os registros que possuem o mesmo nome, o mesmo tipo (como A ou AAAA) e a mesma política de roteamento (como ponderada ou latência) ficam ativos, a menos que o Route 53 os considere não íntegros. O Route 53 pode responder a uma consulta de DNS usando qualquer registro íntegro.

Failover ativo/passivo

Use uma configuração de failover ativo-passivo quando você quiser que um recurso ou um grupo principal de recursos permaneça disponível na maior parte do tempo e um grupo de recursos secundário fique em modo de espera, caso todos os recursos principais estejam indisponíveis.

Ao responder às consultas, o Route 53 inclui somente os recursos principais íntegros. Se nenhum recurso primário estiver íntegro, o Route 53 começará a incluir apenas os recursos secundários íntegros em resposta às consultas de DNS.

Tópicos

Configurar failover ativo/passivo com um recurso principal e um recurso secundário

Para criar uma configuração de failover ativo-passivo com um registro primário e um registro secundário, basta criar os registros e especificar Failover para a política de roteamento. Quando o recurso principal estiver íntegro, o Route 53 responderá às consultas de DNS usando o registro primário. Quando o recurso principal não estiver íntegro, o Route 53 responderá às consultas de DNS usando o registro secundário.

Configurar failover ativo/passivo com vários recursos principais e secundários

Você também pode associar vários recursos ao registro primário, ao registro secundário ou a ambos. Nesta configuração, o Route 53 considerará que o registro de failover primário é íntegro, desde que pelo menos um dos recursos associados seja íntegro também. Para obter mais informações, consulte Como o Amazon Route 53 escolhe registros quando a verificação de integridade está configurada.

Para configurar o failover ativo-passivo com vários recursos para o registro primário ou secundário, execute as seguintes tarefas.

1. Crie uma verificação de integridade para cada recurso ao qual você deseja rotear o tráfego, como uma instância do EC2 ou um servidor web no seu data center.

> **Note**
>
> Se você estiver encaminhando o tráfego para qualquer recurso da AWS para o qual seja possível criar registros com alias, não crie verificações de integridade para esses recursos. Em vez disso, ao criar os registros com alias, defina Evaluate Target Health como Yes.

Para obter mais informações, consulte Criar e atualizar verificações de integridade.

2. Crie registros para seus recursos primários e especifique os seguintes valores:
   - Atribua a cada registro nome, tipo e política de roteamento iguais. Por exemplo, você pode criar três registros A ponderados, todos denominados failover-primary.example.com.
   - Se estiver usando recursos da AWS para os quais você pode criar registros com alias, especifique Yes (Sim) para Evaluate Target Health (Avaliar integridade do destino).

     Se você estiver usando recursos para os quais não é possível criar registros com alias, associe a cada registro a verificação de integridade aplicável da etapa 1.

   Para obter mais informações, consulte Criar registros usando o console do Amazon Route 53.
3. Crie registros para seus recursos secundários, se aplicável, e especifique os seguintes valores:
   - Atribua a cada registro nome, tipo e política de roteamento iguais. Por exemplo, você pode criar três registros A ponderados, todos denominados failover-secondary.example.com.
   - Se estiver usando recursos da AWS para os quais você pode criar registros com alias, especifique Yes (Sim) para Evaluate Target Health (Avaliar integridade do destino).

     Se você estiver usando recursos para os quais não é possível criar registros com alias, associe a cada registro a verificação de integridade aplicável da etapa 1.

   > **Note**
   >
   > Alguns clientes usam um servidor Web como recurso principal e um bucket do Amazon S3 configurado como um endpoint do site como recurso secundário. O bucket do S3 contém uma mensagem simples "temporariamente indisponível". Se você estiver usando essa configuração, poderá ignorar esta etapa e criar um registro de failover com alias para o recurso secundário na etapa 4.

4. Crie dois registros de failover com alias, um primário e um secundário, e especifique os seguintes valores:

   Registro primário
   - Name (Nome): especifique o nome do domínio (example.com) ou o nome do subdomínio (www.example.com) para o qual você deseja que o Route 53 encaminhe o tráfego.
   - Alias: especifique Yes (Sim).
   - Alias Target (Destino do alias): especifique o nome dos registros que você criou na etapa 2.

- Routing Policy (Política de roteamento): especifique Failover.
- Failover Record Type (Tipo de registro de failover): especifique Primary (Primário).
- Evaluate Target Health (Avaliar integridade de destino): especifique Yes (Sim).
- Associate with Health Check (Associar à verificação de integridade): especifique No (Não).

Registro secundária

- Name (Nome): especifique o mesmo nome que você especificou para o registro primário.
- Alias: especifique Yes (Sim).
- Alias Target (Destino do alias): se você tiver criado registros para seu recurso secundário na etapa 3, especifique o nome dos registros. Se você estiver usando um bucket do Amazon S3 para o recurso secundário, especifique o nome DNS do endpoint do site.
- Routing Policy (Política de roteamento): especifique Failover.
- Failover Record Type (Tipo de registro de failover): especifique Secondary (Secundário).
- Evaluate Target Health (Avaliar integridade de destino): especifique Yes (Sim).
- Associate with Health Check (Associar à verificação de integridade): especifique No (Não).

Configurar failover ativo/passivo com registros ponderados

Você também pode usar registros ponderados para failover ativo-passivo, com restrições. Se você especificar pesos diferentes de zero para alguns registros e pesos iguais a zero para outros registros, o Route 53 responderá às consultas de DNS usando somente registros íntegros que tenham pesos diferentes de zero. Se nenhum dos registros com ponderação maior que 0 estiver íntegro, o Route 53 responderá às consultas usando os registros com ponderação igual a zero.

> **Note**
>
> Todos os registros com pesos diferentes de zero precisam ser não íntegros para que o Route 53 comece a responder às consultas de DNS usando registros com pesos iguais a zero. Isso pode tornar seu aplicativo web ou site não confiável se o último recurso íntegro, como um servidor web, não puder lidar com todo o tráfego quando outros recursos estiverem indisponíveis.

Configurar failover em uma zona hospedada privada

Se estiver criando registros de failover em uma zona hospedada privada, observe o seguinte:

- Os verificadores de integridade do Route 53 estão fora da VPC. Para verificar a integridade de um endpoint dentro de uma VPC por endereço IP, você precisa atribuir um endereço IP público à instância na VPC.
- Você pode criar uma métrica do CloudWatch, associar um alarme à métrica e, em seguida, criar uma verificação de integridade baseada no fluxo de dados do alarme. Por exemplo, você pode criar uma métrica do CloudWatch que verifica o status da métrica `StatusCheckFailed` do EC2, adicionar um alarme à métrica e, em seguida, criar uma verificação de integridade com base no fluxo de dados do alarme para verificar instâncias dentro de uma Virtual Private Cloud (VPC) que tem apenas endereços IP privados. Para obter informações sobre como criar métricas e alarmes do CloudWatch usando o console do CloudWatch, consulte o Guia do usuário do Amazon CloudWatch.

Para obter mais informações, consulte Trabalhar com zonas hospedadas privadas e Como monitorar as verificações de integridade usando o CloudWatch.

Como o Amazon Route 53 evita problemas de failover

Os algoritmos de failover implementados pelo Route 53 destinam-se não apenas a direcionar o tráfego para endpoints saudáveis, mas também ajudam a diminuir o risco de desastres por erros de configuração de verificações de integridade e aplicações, sobrecarga de endpoints e falhas de partição.

Tópicos

- Como o Amazon Route 53 evita falhas em cascata
- Como o Amazon Route 53 lida com partições da Internet

Como o Amazon Route 53 evita falhas em cascata

Como primeira defesa contra falhas em cascata, cada algoritmo do roteamento de solicitação (como ponderado e de failover) tem um modo de último recurso. Nesse modo especial, quando todos os registros não são considerados íntegros, o algoritmo do Route 53 é revertido para considerar todos os registros como íntegros.

Por exemplo, se todas as instâncias de uma aplicação, em vários hosts, estiverem rejeitando solicitações de verificação de integridade, os servidores DNS do Route 53 escolherão uma resposta e a retornarão, em vez de não retornar nenhuma resposta DNS ou retornar uma resposta

NXDOMAIN (domínio inexistente). Um aplicativo pode responder aos usuários e ainda falhar nas verificações de integridade. Isso oferece alguma proteção contra configurações incorretas.

Da mesma forma, se uma aplicação estiver sobrecarregada e um dos três endpoints apresentar falha nas verificações de integridade, de modo que seja excluído das respostas DNS do Route 53, o Route 53 distribuirá respostas entre os dois endpoints restantes. Se os endpoints restantes não conseguirem lidar com a carga adicional e falharem, o Route 53 reverterá para distribuir as solicitações aos três endpoints.

Como o Amazon Route 53 lida com partições da Internet

Embora isso seja incomum, há partições da Internet ocasionalmente significativas, o que significa que grandes regiões geográficas não podem se comunicar entre si por meio da Internet. Durante essas partições, os locais do Route 53 podem chegar a conclusões diferentes sobre o status de integridade de um endpoint, e eles podem ser diferentes do status relatado para o CloudWatch. Os verificadores de integridade do Route 53 em cada região da AWS estão constantemente enviando status da verificação de integridade a todos os locais do Route 53. Durante as partições da Internet, cada local do Route 53 pode ter acesso somente a um conjunto parcial desses status, geralmente das regiões mais próximas.

Por exemplo, durante uma partição da Internet que afeta a conectividade para a América do Sul e vice-versa, os servidores DNS do Route 53 no local América do Sul (São Paulo) do Route 53 podem ter um bom acesso aos endpoints de verificação de integridade na região América do Sul (São Paulo) da AWS, mas acesso inadequado a endpoints em outros lugares. Ao mesmo tempo, o Route 53 no Leste dos EUA (Ohio) pode ter acesso inadequado aos endpoints de verificação de integridade na região América do Sul (São Paulo) e concluir que os registros correspondentes não estão íntegros.

Partições como estas podem dar origem a situações em que os locais do Route 53 tiram conclusões diferentes sobre o status de integridade dos endpoints, com base na visibilidade local desses endpoints. É por isso que cada local do Route 53 considera um endpoint íntegro quando somente uma parte dos verificadores de integridade o consideram íntegro.

Nomear e adicionar tags às verificações de integridade

Você pode adicionar tags às verificações de integridade do Amazon Route 53, que permite fornecer a cada verificação de integridade um nome que seja mais abrangente do que um ID de verificação de integridade. Essas são as mesmas etiquetas AWS Billing and Cost Management

que permitem organizar sua AWS fatura. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custos para relatórios de faturamento personalizados no Manual do usuário do AWS Billing .

Cada tag consiste em uma chave (nome da tag) e um valor da tag, ambos definidos por você. Quando você adiciona tags a uma verificação de integridade, recomendamos a inclusão de uma tag que tenha os seguintes valores para a chave e o valor:

- key (chave: Name (Nome)
- value (valor): o nome que você deseja atribuir à verificação de integridade

O valor da tag Name (Nome) é exibido na lista de verificações de integridade, no console do Route 53. Com isso, é possível distinguir prontamente as verificações de integridade umas das outras. Se quiser ver outras tags para uma verificação de integridade, escolha a verificação de integridade e, em seguida, a guia Tags.

Para obter mais informações sobre tags, consulte os tópicos a seguir:

- Para adicionar, editar ou excluir a tag Name (Nome) ao adicionar ou editar verificações de integridade no console do Route 53, consulte Criar, atualizar e excluir verificações de integridade.
- Para obter uma visão geral sobre como marcar recursos do Route 53, consulte Marcação de recursos do Amazon Route 53.

Restrições de tags

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso – 50
- Comprimento máximo da Key (Chave): 128 caracteres Unicode
- Comprimento máximo de Value (Value): 256 caracteres Unicode
- Valores válidos para Key (Chave) e Value (Valor) letras maiúsculas e minúsculas no conjunto de caracteres UTF-8, números, espaço e os seguintes caracteres: _ . : / = + - and @
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas
- Não use o `aws:` prefixo para chaves ou valores; ele está reservado para AWS uso

Adicionar, editar e excluir tags nas verificações de integridade

Os procedimentos a seguir mostram como usar tags nas suas verificações de integridade por meio do console do Route 53.

Tópicos

Para adicionar tags às verificações de integridade (console)

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Selecione uma ou várias verificações de integridade (se desejar adicionar a mesma tag a mais de uma verificação de integridade).
4. No painel inferior, selecione a guia Tags e clique em Adicionar/editar tags.
5. Na caixa de diálogo Adicionar/editar tags, insira um nome para a tag no campo Chave e um valor no campo Valor.
6. Selecione Aplicar alterações.

Para editar tags nas verificações de integridade (console)

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Selecione uma verificação de integridade.

   Se você selecionar várias verificações de integridade que compartilham a mesma tag, não será possível editar o valor de todas as tags simultaneamente. No entanto, você poderá editar o valor de uma tag que aparece em várias verificações de integridade se selecionar verificações de integridade que contêm a tag e pelo menos uma que não a contém.

Por exemplo, suponha que você selecione várias verificações de integridade que têm uma tag Cost Center (Centro de custo) e outra que não tem. Você escolhe a opção de adicionar uma tag e especifica Cost Center (Centro de custo) para a chave, e 777 para o valor. Para verificações de integridade selecionadas que já têm uma tag Cost Center (Centro de custo), o Route 53 altera o valor para 777. Para uma verificação de integridade que não tem uma tag Cost Center (Centro de custo), o Route 53 acrescenta uma e define o valor para 777.

4. No painel inferior, selecione a guia Tags e clique em Adicionar/editar tags.
5. Na caixa de diálogo Adicionar/editar tags, edite o valor.
6. Selecione Save (Salvar).

Para excluir tags nas verificações de integridade (console)

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, selecione Verificações de integridade.
3. Selecione uma ou várias verificações de integridade (se desejar excluir a mesma tag de mais de uma verificação de integridade).
4. No painel inferior, selecione a guia Tags e clique em Adicionar/editar tags.
5. Na caixa de diálogo Adicionar/editar tags, clique no *X* ao lado da tag que você deseja excluir.
6. Selecione Save (Salvar).

Como usar verificações de integridade com versões da API do Amazon Route 53 anteriores a 2012-12-12

As verificações de integridade possuem suporte a partir da versão 2012-12-12 da API do Amazon Route 53. Se uma zona hospedada contiver registros para os quais as verificações de integridade estiverem configuradas, recomendamos que você use somente a API 2012-12-12 ou posterior. Observe as seguintes restrições no uso de verificações de integridade com versões anteriores da API.

- A ação `ChangeResourceRecordSets` não pode criar nem excluir registros que incluem os elementos `EvaluateTargetHealth`, `Failover` ou `HealthCheckId`.

- A ação `ListResourceRecordSets` pode listar registros que incluem esses elementos, mas os elementos não são incluídos na saída. Em vez disso, o elemento `Value` da resposta contém uma mensagem indicando que o registro inclui um atributo sem suporte.

Firewall de DNS do Route 53 Resolver

Com o Firewall DNS do Route 53 Resolver, você pode filtrar e regular o tráfego DNS de saída para sua nuvem privada virtual (VPC). Para fazer isso, você cria coleções reutilizáveis de regras de filtragem em grupos de regras do Firewall DNS, associa os grupos de regras à sua VPC e monitora a atividade em logs e métricas do Firewall DNS. Com base na atividade, você pode ajustar o comportamento do Firewall DNS adequadamente.

O Firewall DNS fornece proteção para solicitações DNS de saída de suas VPCs. Essas solicitações são encaminhadas através do Resolver para resolução de nomes de domínio. Um uso principal das proteções do Firewall DNS é ajudar a impedir a exfiltração de DNS de seus dados. A exfiltração de DNS pode ocorrer quando um ator proibido compromete uma instância da aplicação em sua VPC e, em seguida, usa a pesquisa DNS para enviar dados da VPC para um domínio que eles controlam. Com o Firewall DNS, você pode monitorar e controlar os domínios que as aplicações podem consultar. Você pode negar acesso aos domínios que você sabe que são incorretos e permitir que todas as outras consultas passem. Como alternativa, você pode negar acesso a todos os domínios, exceto aqueles em que você confia explicitamente.

Você também pode usar o Firewall DNS para bloquear solicitações de resolução para recursos em zonas hospedadas privadas (compartilhadas ou locais), incluindo nomes de endpoint da VPC. Ele também pode bloquear solicitações de nomes de instâncias públicas ou privadas do Amazon EC2.

O Firewall DNS é um recurso do Route 53 Resolver e não requer nenhuma configuração adicional do Resolver para usar.

AWS Firewall Manager suporta DNS Firewall

Você pode usar o Firewall Manager para configurar e gerenciar centralmente suas associações de grupos de regras do Firewall DNS para suas VPCs em suas contas no AWS Organizations. O Firewall Manager adiciona automaticamente associações para VPCs que entram no escopo de sua política de Firewall DNS do Firewall Manager. Para obter mais informações, consulte AWS Firewall Managerno AWS WAF, AWS Firewall Manager, e no Guia AWS Shield Advanced do desenvolvedor.

Como o DNS Firewall funciona com AWS Network Firewall

O Firewall DNS e o Network Firewall oferecem filtragem de nomes de domínio, mas para diferentes tipos de tráfego. Com o Firewall DNS e o Network Firewall juntos, você pode configurar a filtragem baseada em domínio para o tráfego da camada de aplicação em dois caminhos de rede diferentes.

- O Firewall DNS fornece filtragem para consultas de DNS de saída que passam pelo Route 53 Resolver a partir de aplicações dentro de suas VPCs. Você também pode configurar o Firewall DNS para enviar respostas personalizadas para consultas a nomes de domínio bloqueados.
- O Network Firewall fornece filtragem para tráfego de camada de rede e aplicação, mas não tem visibilidade em consultas feitas pelo Route 53 Resolver.

Para obter mais informações sobre Network Firewall, consulte o Guia do desenvolvedor do Network Firewall.

Como o Firewall DNS do Route 53 Resolver funciona

O Firewall DNS do Route 53 Resolver permite controlar o acesso a sites e bloquear ameaças no nível de DNS para consultas de DNS que saem da sua VPC através do Route 53 Resolver. Com o Firewall DNS, você define regras de filtragem de nomes de domínio em grupos de regras que você associa às VPCs. Você pode especificar listas de nomes de domínio para permitir ou bloquear e personalizar as respostas para as consultas DNS que você bloqueia. Você também pode ajustar as listas de domínios para permitir a passagem de determinados tipos de consulta, como registros MX.

O Firewall DNS filtra apenas o nome de domínio. Ele não resolve esse nome para um endereço IP a ser bloqueado. Além disso, o DNS Firewall filtra o tráfego DNS, mas não filtra outros protocolos da camada de aplicativos, como HTTPS, SSH, TLS, FTP e assim por diante.

Componentes e configurações do Firewall DNS do Route 53 Resolver

Você gerencia o Firewall DNS com os seguintes componentes centrais e configurações.

Grupo de regras do Firewall DNS

Define uma coleção nomeada e reutilizável de regras de Firewall DNS para filtrar consultas de DNS. Preencha o grupo de regras com as regras de filtragem e, em seguida, associe o grupo de regras a uma ou mais VPCs. Quando você associa um grupo de regras a uma VPC, você habilita a filtragem do Firewall DNS para a VPC. Em seguida, quando o Resolver recebe uma consulta de DNS para uma VPC que tenha um grupo de regras associado a ela, ele passa a consulta para o Firewall DNS para filtragem.

Se você associar vários grupos de regras a uma única VPC, indique sua ordem de processamento por meio da configuração de prioridade em cada associação. O Firewall DNS

processa grupos de regras para uma VPC a partir da configuração de prioridade numérica mais baixa para alta.

Para ter mais informações, consulte Regras e grupos de regras do Firewall DNS.

Regra do Firewall DNS

Define uma regra de filtragem para consultas de DNS em um grupo de regras do Firewall DNS. Cada regra especifica uma lista de domínios e uma ação a ser executada em consultas de DNS cujos domínios correspondem às especificações de domínio na lista. Você pode permitir, bloquear ou alertar sobre consultas ou tipos de consulta correspondentes para os domínios na lista. Por exemplo, você pode bloquear ou permitir um tipo de consulta MX para um domínio ou domínios específicos. Você também pode definir respostas personalizadas para consultas bloqueadas.

Cada regra em um grupo de regras tem uma configuração de prioridade exclusiva dentro do grupo de regras. O Firewall DNS processa as regras em um grupo de regras por ordem de prioridade, começando pela configuração mais baixa.

As regras do Firewall DNS existem apenas no contexto do grupo de regras no qual estão definidas. Não é possível reutilizar uma regra ou referenciá-la independentemente do grupo de regras.

Para ter mais informações, consulte Regras e grupos de regras do Firewall DNS.

Lista de domínios

Define uma coleção nomeada e reutilizável de especificações de domínio para uso na filtragem DNS. Cada regra em um grupo de regras requer uma única lista de domínios. Você pode optar por especificar os domínios aos quais deseja permitir acesso, os domínios aos quais deseja negar acesso ou uma combinação de ambos. Você pode criar suas próprias listas de domínios e usar listas de domínios que AWS gerenciam para você.

Para ter mais informações, consulte Listas de domínios do Firewall DNS do Route 53 Resolver.

Configuração de redirecionamento de domínio

A configuração de redirecionamento de domínio permite que você configure uma regra de firewall de DNS para inspecionar todos os domínios na cadeia de redirecionamento de DNS (padrão), como CNAME, DNAME etc., ou apenas o primeiro domínio e confie no resto. Se você optar por inspecionar toda a cadeia de redirecionamento de DNS, deverá adicionar os domínios subsequentes a uma lista de domínios definida como PERMITIR na regra. Se você optar por inspecionar toda a cadeia de redirecionamento de DNS, deverá adicionar os domínios

subsequentes a uma lista de domínios e definir a ação que deseja que a regra execute, seja PERMITIR, BLOQUEAR ou ALERTAR.

Para ter mais informações, consulte Configurações de regra no Firewall DNS.

Tipo da consulta

A configuração do tipo de consulta permite que você configure uma regra de firewall de DNS para filtrar um determinado tipo de consulta de DNS. Se você não selecionar um tipo de consulta, a regra será aplicada a todos os tipos de consulta DNS. Por exemplo, talvez você queira bloquear todos os tipos de consulta de um domínio específico, mas permitir registros MX.

Para ter mais informações, consulte Configurações de regra no Firewall DNS.

Associação entre um grupo de regras do Firewall DNS e uma VPC

Define uma proteção para uma VPC usando um grupo de regras do Firewall DNS e habilita a configuração do Firewall DNS do Resolver para a VPC.

Se você associar vários grupos de regras a uma única VPC, indique sua ordem de processamento por meio da configuração de prioridade nas associações. O Firewall DNS processa grupos de regras para uma VPC a partir da configuração de prioridade numérica mais baixa para alta.

Para ter mais informações, consulte Como habilitar as proteções do Firewall DNS do Route 53 Resolver para a VPC.

Configuração do Firewall DNS do Resolver para uma VPC

Especifica como o Resolver deve lidar com as proteções do Firewall DNS no nível da VPC. Essa configuração terá efeito sempre que você tiver pelo menos um grupo de regras do Firewall DNS associado à VPC.

Essa configuração especifica como o Route 53 Resolver lida com consultas quando o Firewall DNS não consegue filtrá-las. Por padrão, se o Resolver não receber uma resposta do Firewall DNS para uma consulta, ele não será fechado e bloqueará a consulta.

Para ter mais informações, consulte Configuração da VPC do Firewall DNS.

Monitorando ações do firewall DNS

Você pode usar CloudWatch a Amazon para monitorar o número de consultas de DNS que são filtradas por grupos de regras do DNS Firewall. CloudWatch coleta e processa dados brutos em métricas legíveis e quase em tempo real.

Para ter mais informações, consulte Monitorando grupos de regras do firewall DNS do Route 53 Resolver com a Amazon CloudWatch.

Você pode usar a Amazon EventBridge, um serviço sem servidor que usa eventos para conectar componentes do aplicativo e criar aplicativos escaláveis orientados por eventos.

Para ter mais informações, consulte Gerenciando eventos do Route 53 Resolver DNS Firewall usando Amazon EventBridge.

Como o Firewall DNS do Route 53 Resolver filtra consultas de DNS

Quando um grupo de regras de Firewall DNS está associado ao Route 53 Resolver da VPC, o seguinte tráfego é filtrado pelo firewall:

- Consultas de DNS originadas nessa VPC.
- Consultas de DNS que passam por endpoints do Resolver de recursos on-premises para a mesma VPC que tem o DNS Firewall associado ao seu resolvedor.

Quando o Firewall DNS recebe uma consulta de DNS, ele filtra a consulta usando os grupos de regras, regras e outras configurações que você configurou e envia os resultados de volta para o Resolver:

- O Firewall DNS avalia a consulta de DNS usando os grupos de regras associados à VPC até encontrar uma correspondência ou esgotar todos os grupos de regras. O Firewall DNS avalia os grupos de regras na ordem da prioridade que você definiu na associação, começando com a configuração numérica mais baixa. Para obter mais informações, consulte Regras e grupos de regras do Firewall DNS e Como habilitar as proteções do Firewall DNS do Route 53 Resolver para a VPC.
- Dentro de cada grupo de regras, o Firewall DNS avalia a consulta de DNS em relação à lista de domínios de cada regra até encontrar uma correspondência ou esgotar todas as regras. O DNS Firewall avalia as regras em ordem de prioridade, começando com a configuração numérica mais baixa. Para ter mais informações, consulte Regras e grupos de regras do Firewall DNS.
- Quando o Firewall DNS encontra uma correspondência com a lista de domínios de uma regra, ele encerra a avaliação da consulta e responde ao Resolver com o resultado. Se a ação for `alert`, o Firewall DNS também envia um alerta para os logs do Resolver configurados. Para obter mais informações, consulte Ações de regra no Firewall DNS e Listas de domínios do Firewall DNS do Route 53 Resolver.

- Se o Firewall DNS avaliar todos os grupos de regras sem encontrar uma correspondência, ele responderá à consulta normalmente.

O Resolver encaminhará a consulta, de acordo com a resposta do Firewall DNS. No caso improvável de que o Firewall DNS não responda, o Resolver aplicará o modo de falha do Firewall DNS configurado da VPC. Para ter mais informações, consulte Configuração da VPC do Firewall DNS.

Etapas de nível superior para usar o Firewall DNS do Route 53 Resolver

Para implementar a filtragem do Firewall DNS do Route 53 Resolver na Amazon Virtual Private Cloud VPC, execute as seguintes etapas de alto nível.

- Definir sua abordagem de filtragem e suas listas de domínio: decida como você deseja filtrar consultas, identifique as especificações de domínio necessárias e defina a lógica que você usará para avaliar consultas. Por exemplo, talvez você queira permitir todas as consultas, exceto aquelas que estão em uma lista de domínios inválidos conhecidos. Ou você pode querer fazer o oposto e bloquear todos, exceto uma lista aprovada de domínios, no que é conhecido como uma abordagem de jardim murado. Você pode criar e gerenciar suas próprias listas de especificações de domínio aprovadas ou bloqueadas e usar listas de domínios que AWS gerenciam para você. Para obter informações sobre listas de domínios, consulte. Listas de domínios do Firewall DNS do Route 53 Resolver
- Criar um grupo de regras de firewall: no Firewall DNS, crie um grupo de regras para filtrar consultas de DNS para sua VPC. Você deve criar um grupo de regras em cada região onde deseja usá-lo. Você também pode querer separar seu comportamento de filtragem em mais de um grupo de regras para reutilização em vários cenários de filtragem para suas diferentes VPCs. Para obter informações sobre grupos de regras, consulte Regras e grupos de regras do Firewall DNS.
- Adicionar e configurar suas regras: adicione uma regra ao grupo de regras para cada lista de domínios e comportamento de filtragem que você deseja que o grupo de regras forneça. Defina as configurações de prioridade para suas regras para que elas sejam processadas na ordem correta dentro do grupo de regras, dando a prioridade mais baixa à regra que você deseja avaliar primeiro. Para obter mais informações sobre regras, consulte Regras e grupos de regras do Firewall DNS.
- Associar o grupo de regras à sua VPC: para começar a usar o grupo de regras do Firewall DNS, associe-o à sua VPC. Se você estiver usando mais de um grupo de regras para sua VPC, defina a prioridade de cada associação para que os grupos de regras sejam processados na ordem correta, dando a prioridade mais baixa ao grupo de regras que você deseja avaliar primeiro. Para

ter mais informações, consulte Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver.

- (Opcional) Alterar a configuração do firewall para a VPC: se você deseja que o Route 53 Resolver bloqueie consultas quando o Firewall DNS não enviar uma resposta para elas, no Resolver, altere a configuração do Firewall DNS da VPC. Para ter mais informações, consulte Configuração da VPC do Firewall DNS.

Como usar grupos de regras do Firewall DNS do Route 53 Resolver em várias regiões

O Route 53 Resolver DNS Firewall é um serviço regional, portanto, os objetos que você cria em uma AWS região estão disponíveis somente nessa região. Para usar o mesmo grupo de regras em mais de uma região, é necessário criar a regra em cada região.

A AWS conta que criou um grupo de regras pode compartilhá-lo com outras AWS contas. Para ter mais informações, consulte Compartilhando grupos de regras do Route 53 Resolver DNS Firewall entre contas AWS.

Conceitos básicos do Firewall DNS do Route 53 Resolver

O console do Firewall DNS inclui um assistente que orienta você durante as etapas a seguir para começar a usar o Firewall DNS:

- Crie grupos de regras para cada conjunto de regras que você deseja usar.
- Para cada regra, preencha a lista de domínios que você deseja inspecionar. Você pode criar suas próprias listas de domínios e usar listas de domínios AWS gerenciados.
- Associe seus grupos de regras às VPCs onde deseja usá-los.

Exemplo do jardim murado do Firewall DNS do Route 53 Resolver

Neste tutorial, você criará um grupo de regras que bloqueia todos, exceto um grupo selecionado, de domínios nos quais você confia. Isso é chamado de plataforma fechada, ou abordagem de jardim murado.

Para configurar um grupo de regras do Firewall DNS usando o assistente de console

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 3.

   - OU -

   Faça login no AWS Management Console e abra o

   o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.
4. Na página Rule groups (Grupos de regras), escolha Add rule group (Adicionar grupo de regras).
5. Para o nome do grupo de regras, insira **`WalledGardenExample`**.

   Na seção Tags, você pode, opcionalmente, inserir um par de valores-chave para uma tag. As tags ajudam você a organizar e gerenciar seus recursos do AWS . Para ter mais informações, consulte Marcação de recursos do Amazon Route 53.
6. Escolha Adicionar grupo de regras.
7. Na página Detalhes do WalledGardenexemplo, escolha a guia Regras e, em seguida, Adicionar regra.
8. No painel Rule details (Detalhes da regra), insira o nome da regra **`BlockAll`**.
9. No painel Domain list (Lista de domínios), selecione Add my own domain list (Adicionar minha própria lista de domínios).
10. Em Choose or create a new domain list (Escolher ou criar uma lista de domínios) escolha Create new domain list (Criar nova lista de domínios).
11. Insira o nome da lista de domínios e**`AllDomains`**, na caixa de texto Inserir um domínio por linha, insira um asterisco:**`*`**.
12. Para a configuração de redirecionamento de domínio, aceite o padrão e deixe o tipo de consulta - opcional em branco.
13. Para a Ação, selecione BLOQUEAR e, em seguida, deixe a resposta ser enviada na configuração padrão de NODATA.

14. Escolha Adicionar regra. Sua regra BlockAllé exibida na guia Regras na página WalledGardenExemplo.
15. Na página WalledGardenExemplo, escolha Adicionar regra para adicionar uma segunda regra ao seu grupo de regras.
16. No painel Detalhes da regra, insira o nome **`AllowSelectDomains`** da regra.
17. No painel Domain list (Lista de domínios), selecione Add my own domain list (Adicionar minha própria lista de domínios).
18. Em Choose or create a new domain list (Escolher ou criar uma nova lista de domínios), selecione Create new domain list (Criar nova lista de domínios).
19. Insira um nome de lista de domínios **`ExampleDomains`**.
20. Na caixa de texto Inserir um domínio por linha, na primeira linha, insira **`example.com`** e, na segunda linha, insira**`example.org`**.

    > **Note**
    >
    > Se você quiser que a regra se aplique a subdomínios também, você precisa adicionar esses domínios à lista também. Por exemplo, para adicionar todos os subdomínios do example.com, adicione **`*.example.com`** à lista.

21. Para a configuração de redirecionamento de domínio, aceite o padrão e deixe o tipo de consulta - opcional em branco.
22. Para a Ação, selecione PERMITIR.
23. Escolha Adicionar regra. Suas regras são exibidas na guia Regras na página WalledGardenExemplo.
24. Na guia Regras na página WalledGardenExemplo, você pode ajustar a ordem de avaliação das regras em seu grupo de regras selecionando o número listado na coluna Prioridade e digitando um novo número. O DNS Firewall avalia as regras começando com a configuração de prioridade mais baixa, portanto, a regra com a prioridade mais baixa é a primeira a ser avaliada. Para este exemplo, queremos que o Firewall DNS primeiro identifique e permita consultas de DNS para a lista selecionada de domínios e, em seguida, bloqueie todas as consultas restantes.

    Ajuste a prioridade da regra para que AllowSelectos domínios tenham uma prioridade menor.

Agora você tem um grupo de regras que permite apenas consultas de domínio específicas. Para começar a usá-lo, associe-o às VPCs nas quais deseja usar o comportamento de filtragem. Para

ter mais informações, consulte Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver.

Exemplo da lista de bloqueios do Firewall DNS do Route 53 Resolver

Neste tutorial, você criará um grupo de regras que bloqueia domínios que você sabe que são maliciosos. Você também adicionará um tipo de consulta DNS que é permitido para os domínios na lista bloqueada. O grupo de regras permite todas as outras solicitações DNS de saída pelo Route 53 Resolver.

Para configurar uma lista de bloqueios do Firewall DNS utilizando o assistente do console

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 3.

   - OU -

   Faça login AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.
4. Na página Rule groups (Grupos de regras), escolha Add rule group (Adicionar grupo de regras).
5. Para o nome do grupo de regras, insira **`BlockListExample`**.

   Na seção Tags, você pode, opcionalmente, inserir um par de valores-chave para uma tag. As tags ajudam você a organizar e gerenciar seus recursos do AWS . Para ter mais informações, consulte Marcação de recursos do Amazon Route 53.
6. Na página Detalhes do BlockListexemplo, escolha a guia Regras e, em seguida, Adicionar regra.
7. No painel Rule details (Detalhes da regra), insira o nome da regra **`BlockList`**.
8. No painel Domain list (Lista de domínios), selecione Add my own domain list (Adicionar minha própria lista de domínios).
9. Em Choose or create a new domain list (Escolher ou criar uma nova lista de domínios), selecione Create new domain list (Criar nova lista de domínios).

10. Insira um nome de lista de domínios **`MaliciousDomains`**, em seguida, na caixa de texto, insira os domínios que você deseja bloquear. Por exemplo, **`example.org`**. Insira um domínio por linha.

    > **Note**
    >
    > Se você quiser que a regra se aplique a subdomínios também, você deve adicionar esses domínios à lista também. Por exemplo, para adicionar todos os subdomínios do example.org, adicione**`*.example.org`** à lista.

11. Para a configuração de redirecionamento de domínio, aceite o padrão e deixe o tipo de consulta - opcional em branco.
12. Para a ação, selecione BLOCK (Bloquear) e, em seguida, deixe a resposta para enviar na configuração padrão de NODATA.
13. Escolha Adicionar regra. Sua regra é exibida na guia Regras na página BlockListExemplo
14. na guia Regras na página BlockedListExemplo, você pode ajustar a ordem de avaliação das regras em seu grupo de regras selecionando o número listado na coluna Prioridade e digitando um novo número. O DNS Firewall avalia as regras começando com a configuração de prioridade mais baixa, portanto, a regra com a prioridade mais baixa é a primeira a ser avaliada.

    Selecione e ajuste a prioridade da regra para que ela BlockListseja avaliada antes ou depois de qualquer outra regra que você possa ter. Na maioria das vezes, domínios maliciosos conhecidos devem ser bloqueados primeiro. Ou seja, as regras associadas a elas devem ter o número de prioridade mais baixo.
15. Para adicionar uma regra que permita registros MX para os BlockList domínios, na página Detalhes do BlockedListexemplo, na guia Regras, escolha Adicionar regra.
16. No painel Rule details (Detalhes da regra), insira o nome da regra **`BlockList-allowMX`**.
17. No painel Domain list (Lista de domínios), selecione Add my own domain list (Adicionar minha própria lista de domínios).
18. Em Escolher ou criar uma nova lista de domínios, selecione**`MaliciousDomains`**.
19. Para a configuração de redirecionamento de domínio, aceite o padrão.
20. Na lista de tipos de consulta DNS, selecione MX: Especifica servidores de e-mail.
21. Para a ação, selecione ALLOW (Permitir).
22. Escolha Adicionar regra.

23. na guia Regras na página BlockedListExemplo, você pode ajustar a ordem de avaliação das regras em seu grupo de regras selecionando o número listado na coluna Prioridade e digitando um novo número. O DNS Firewall avalia as regras começando com a configuração de prioridade mais baixa, portanto, a regra com a prioridade mais baixa é a primeira a ser avaliada.

    Selecione e ajuste a prioridade da regra para que BlockList-allowMx seja avaliado antes ou depois de qualquer outra regra que você possa ter. Como você deseja permitir consultas MX, certifique-se de que a regra BlockList-allowMx tenha uma prioridade menor que a. BlockList

Agora você tem um grupo de regras que bloqueia consultas de domínio maliciosas específicas, mas permite um tipo específico de consulta de DNS. Para começar a usá-lo, associe-o às VPCs nas quais deseja usar o comportamento de filtragem. Para ter mais informações, consulte Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver.

Regras e grupos de regras do Firewall DNS

Esta seção descreve as configurações que você pode configurar para os grupos de regras e regras do Firewall DNS para definir o comportamento do Firewall DNS para suas VPCs. Ela também descreve como gerenciar as configurações para seus grupos de regras e regras.

Quando você tiver seus grupos de regras configurados da maneira desejada, você os usa diretamente e poderá compartilhá-los e gerenciá-los entre contas e em toda a organização no AWS Organizations.

- Você pode associar um grupo de regras a várias VPCs para fornecer um comportamento consistente em toda a organização. Para mais informações, consulte Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver.
- Você pode compartilhar grupos de regras entre contas, para gerenciamento consistente de consultas de DNS em toda a organização. Para mais informações, consulte Compartilhando grupos de regras do Route 53 Resolver DNS Firewall entre contas AWS.
- Você pode usar grupos de regras em toda a sua organização AWS Organizations gerenciando-os em AWS Firewall Manager políticas. Para obter informações sobre o Firewall Manager, consulte AWS Firewall Managero AWS WAF AWS Firewall Manager, e o Guia AWS Shield Advanced do Desenvolvedor.

Configurações de grupo de regras no Firewall DNS

Ao criar ou editar um grupo de regras do Firewall DNS, especifique os seguintes valores:

Nome

Um nome exclusivo que permite encontrar facilmente um grupo de regras no painel.

Descrição (opcional)

Uma descrição curta que fornece mais contexto para o grupo de regras.

Região

A AWS região que você escolhe ao criar o grupo de regras. Um grupo de regras criado em uma região só está disponível nessa região. Para usar o mesmo grupo de regras em mais de uma região, é necessário criar a regra em cada região.

Regras

O comportamento de filtragem do grupo de regras está contido em suas regras. Para obter mais informações, consulte a seção a seguir.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Essas são as etiquetas AWS Billing and Cost Management que permitem organizar sua AWS fatura. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing .

Configurações de regra no Firewall DNS

Ao criar ou editar uma regra em um grupo de regras do Firewall DNS, especifique os seguintes valores:

Nome

O identificador exclusivo da regra a ser excluída do grupo de regras.

Descrição (opcional)

Uma breve descrição que fornece mais informações sobre a regra.

Lista de domínios

A lista de domínios que a regra inspeciona. Você pode criar e gerenciar sua própria lista de domínios ou pode se inscrever em uma lista de domínios que a AWS gerencia para você. Para ter mais informações, consulte Listas de domínios do Firewall DNS do Route 53 Resolver.

Configuração de redirecionamento de domínio

Você pode escolher que a regra de firewall de DNS inspecione somente o primeiro domínio ou todos (padrão) os domínios na cadeia de redirecionamento de DNS, como CNAME, DNAME etc. Se você optar por inspecionar todos os domínios, deverá adicionar os domínios subsequentes na cadeia de redirecionamento de DNS à lista de domínios e definir a ação que deseja que a regra execute, seja PERMITIR, BLOQUEAR ou ALERTAR. Para ter mais informações, consulte Componentes e configurações do Firewall DNS do Route 53 Resolver.

Tipo da consulta

A lista de tipos de consulta de DNS que a regra inspeciona. A seguir estão os valores válidos:

- R: Retorna um endereço IPv4.
- AAAA: retorna um endereço Ipv6.
- CAA: restringe CAs que podem criar certificações SSL/TLS para o domínio.
- CNAME: retorna outro nome de domínio.
- DS: Registro que identifica a chave de assinatura DNSSEC de uma zona delegada.
- MX: especifica servidores de e-mail.
- NAPTR: R egular-expression-based reescrita de nomes de domínio.
- NS: servidores de nomes autorizados.
- PTR: mapeia um endereço IP para um nome de domínio.
- SOA: Início do registro de autoridade para a zona.
- SPF: lista os servidores autorizados a enviar e-mails de um domínio.
- SRV: valores específicos do aplicativo que identificam servidores.
- TXT: verifica os remetentes de e-mail e os valores específicos do aplicativo.
- Um tipo de consulta que você define usando o ID do tipo DNS, por exemplo, 28 para AAAA. Os valores devem ser definidos como TYPE *`NUMBER, onde o NUMBER`* pode ser de 1 a 65334, por exemplo, TYPE28. Para obter mais informações, consulte Lista de tipos de registro DNS.

  Você pode criar um tipo de consulta por regra.

> **Note**
>
> Se você configurar uma regra BLOCK de firewall com a ação NXDOMAIN no tipo de consulta igual a AAAA, essa ação não será aplicada aos endereços IPv6 sintéticos gerados quando o DNS64 estiver ativado.

Ação

Como você deseja que o Firewall DNS manipule uma consulta de DNS cujo nome de domínio corresponda às especificações na lista de domínios da regra. Para ter mais informações, consulte Ações de regra no Firewall DNS.

Prioridade

A configuração de inteiro positivo exclusivo para a regra no grupo de regras que determina a ordem de processamento. O DNS Firewall inspeciona consultas de DNS contra as regras em um grupo de regras começando com a configuração de prioridade numérica mais baixa e indo para cima. Você pode alterar a prioridade de uma regra a qualquer momento, por exemplo, para alterar a ordem de processamento ou abrir espaço para outras regras.

Ações de regra no Firewall DNS

Quando o Firewall DNS localiza uma correspondência entre uma consulta de DNS e uma especificação de domínio em uma regra, ele aplica a ação especificada na regra à consulta.

Você tem que especificar uma das seguintes opções em cada regra criada:

- Allow: interrompa a inspeção da consulta e permita que ela passe.
- Alert: interrompa a inspeção da consulta, permita que ela passe e registre um alerta para a consulta nos logs do Route 53 Resolver.
- Block: interrompa a inspeção da consulta, bloqueie-a de ir para o destino pretendido e registre a ação de bloqueio para a consulta nos logs do Route 53 Resolver.

  Responda com a resposta de bloco configurada, a partir do seguinte:

  - NODATA: responde indicando que a consulta foi bem-sucedida, mas nenhuma resposta está disponível para ela.
  - NXDOMAIN: responda indicando que o nome do domínio que está na consulta não existe.

- OVERRIDE: fornece uma substituição personalizada na resposta. Além disso, essa instrução requer as seguintes configurações:
  - Record value: o registro DNS personalizado a ser enviado de volta em resposta à consulta.
  - Record type: o tipo do registro DNS. Isso determina o formato do valor do registro. Deve ser `CNAME`.
  - Time to live in seconds: o tempo recomendado para que o resolvedor DNS ou o navegador da Web armazene o registro de substituição e o use em resposta a essa consulta, se ele for recebido novamente. Por padrão, isso é zero e o registro não é armazenado em cache.

Para obter mais informações sobre a configuração dos logs de consulta e o conteúdo, consulte Log de consultas do Resolver e Valores que aparecem em logs de consultas do Resolver.

Usar Alert para testar regras de bloqueio

Quando você cria uma regra de bloqueio pela primeira vez, pode testá-la configurando-a com a ação definida como Alert. Em seguida, você pode examinar o número de consultas nas quais os alertas de regra para ver quantas seriam bloqueadas se você definir a ação como Block.

Como gerenciar grupos de regras e regras no Firewall DNS

Para gerenciar grupos de regras e regras no console, siga as orientações neste tópico.

Quando você faz alterações em entidades do Firewall DNS, como regras e listas de domínios, o Firewall DNS propaga as alterações em todos os lugares em que as entidades são armazenadas e usadas. Suas alterações são aplicadas em segundos, mas pode haver um breve período de inconsistência quando as alterações chegam em alguns lugares e não em outros. Assim, por exemplo, se você adicionar um domínio a uma lista de domínios referenciada por uma regra de bloqueio, o novo domínio poderá ser brevemente bloqueado em uma área da VPC, enquanto ainda é permitido em outra. Essa inconsistência temporária pode ocorrer quando você configura pela primeira vez suas associações de grupo de regras e VPC e quando você altera as configurações existentes. Geralmente, quaisquer inconsistências deste tipo duram apenas alguns segundos.

Criar um grupo de regras e regras

Para criar um grupo de regras e suas regras

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 3.

- OU -

Faça login no AWS Management Console e abra o

o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.
4. Escolha Add rule group (Adicionar grupo de regras) e siga as orientações do assistente para especificar o grupo de regras e as configurações de regras.

   Para obter informações sobre os valores dos grupos de regras, consulte Configurações de grupo de regras no Firewall DNS.

   Para obter informações sobre os valores das regras, consulte Configurações de regra no Firewall DNS.

Como exibir e atualizar um grupo de regras e regras

Para exibir e atualizar um grupo de regras

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 3.

   - OU -

   Faça login no AWS Management Console e abra o

   o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.
4. Selecione o grupo de regras que você deseja exibir ou editar e escolha View details (Exibir detalhes).

5. Na página do grupo de regras, é possível exibir e editar configurações.

   Para obter informações sobre os valores dos grupos de regras, consulte Configurações de grupo de regras no Firewall DNS.

   Para obter informações sobre os valores das regras, consulte Configurações de regra no Firewall DNS.

Excluir um grupo de regras

Para excluir um grupo de regras, execute o procedimento a seguir.

> **Important**
>
> Se você excluir um grupo de regras associado a uma VPC, o Firewall DNS removerá a associação e interromperá as proteções que o grupo de regras estava fornecendo à VPC.

Como excluir entidades do Firewall DNS

Quando você exclui uma entidade que pode usar no Firewall DNS, como uma lista de domínios que pode estar em uso em um grupo de regras ou um grupo de regras que possa estar associado a uma VPC, o Firewall DNS verifica se a entidade está sendo usada no momento. Se ele descobrir que ela está sendo usada, o Firewall DNS avisa. O Firewall DNS quase sempre é capaz de determinar se uma entidade está sendo usada. No entanto, em casos raros, talvez não seja possível fazer isso. Se você precisar ter certeza de que nada está usando a entidade no momento, verifique nas configurações do Firewall DNS antes de excluí-lo. Se a entidade for uma lista de domínios referenciada, verifique se nenhum grupo de regras está utilizando-a. Se a entidade for um grupo de regras, verifique se ela não está associada a nenhuma VPC.

Para excluir um grupo de regras

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 3.

   - OU -

Faça login no AWS Management Console e abra o

o console da Amazon VPC em https://console.aws.amazon.com/vpc/.

2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.
4. Selecione o grupo de regras que você deseja excluir e escolha Delete (Excluir) e confirme a exclusão.

Listas de domínios do Firewall DNS do Route 53 Resolver

Uma lista de domínios é um conjunto reutilizável de especificações de domínios que você usa em uma regra do DNS Firewall, dentro de um grupo de regras. Quando você associa um grupo de regras a uma VPC, o DNS Firewall compara suas consultas de DNS com as listas de domínios usadas nas regras. Se encontrar uma correspondência, ele manipula a consulta de DNS de acordo com a ação da regra correspondente. Para obter mais informações sobre regras e grupos de regras, consulte Regras e grupos de regras do Firewall DNS.

As listas de domínios permitem que você separe suas especificações de domínio explícitas das ações que você deseja executar sobre elas. Você pode usar uma única lista de domínios em várias regras e todas as atualizações feitas na lista de domínios afetam automaticamente todas as regras que a usam.

As listas de domínios se enquadram em duas categorias principais:

- Listas de domínios gerenciados, que AWS criam e mantêm para você.
- Suas próprias listas de domínios, que você cria e mantém.

Esta seção descreve os tipos de grupos de regras gerenciadas que estão disponíveis para você e fornece orientações para criar e gerenciar seus próprios grupos de regras, se você optar por fazê-lo.

Listas de domínios gerenciados

As listas de domínios gerenciados contêm nomes de domínio associados a atividades maliciosas ou outras ameaças em potencial. AWS mantém essas listas para permitir que os clientes do Route 53 Resolver verifiquem as consultas de DNS de saída com eles gratuitamente ao usar o DNS Firewall.

Manter se atualizado sobre o panorama de ameaças em constante alteração pode ser demorado e caro. As listas de domínios gerenciados podem economizar seu tempo ao implementar e usar o Firewall DNS. AWS atualiza automaticamente as listas quando surgem novas vulnerabilidades e ameaças. AWS geralmente é notificado sobre novas vulnerabilidades antes da divulgação pública, portanto, o DNS Firewall pode implantar mitigações para você com frequência antes que uma nova ameaça se torne amplamente conhecida.

As listas de domínios gerenciados destinam-se a ajudar a proteger você contra ameaças comuns da Web e elas adicionam mais uma camada de segurança para as suas aplicações. As listas de domínios AWS gerenciados obtêm seus dados tanto de AWS fontes internas quanto de fontes internas e são atualizadas continuamente. RecordedFuture No entanto, as listas de domínios AWS gerenciados não substituem outros controles de segurança Amazon GuardDuty, como os determinados pelos AWS recursos que você seleciona.

Como prática recomendada, antes de usar uma lista de domínios gerenciada na produção, teste-a em um ambiente que não seja de produção, com a ação da regra definida como `Alert`. Avalie a regra usando CloudWatch métricas da Amazon combinadas com solicitações amostradas do Route 53 Resolver DNS Firewall ou registros do DNS Firewall. Quando você estiver satisfeito de que a regra faz o que você deseja, altere a configuração de ação, conforme necessário.

Listas de domínios AWS gerenciados disponíveis

Esta seção descreve as Listas de domínios gerenciados pela que estão disponíveis atualmente. Quando estiver em uma região compatível com essas listas de domínios, você as verá no console quando gerenciar listas de domínios e quando especificar a lista de domínios para uma regra. Nos logs, a lista de domínios é registrada dentro do`firewall_domain_list_id field`.

AWS fornece as seguintes listas de domínios gerenciados, nas regiões em que estão disponíveis, para todos os usuários do firewall DNS do Route 53 Resolver.

- `AWSManagedDomainsMalwareDomainList`: domínios associados ao envio de malware, hospedagem de malware ou distribuição de malware.
- `AWSManagedDomainsBotnetCommandandControl`: domínios associados ao controle de redes de computadores infectados com malware de spam.
- `AWSManagedDomainsAggregateThreatList`— Domínios associados a várias categorias de ameaças de DNS, incluindo malware, ransomware, botnet, spyware e tunelamento de DNS para ajudar a bloquear vários tipos de ameaças. `AWSManagedDomainsAggregateThreatList`inclui todos os domínios nas outras listas de domínios AWS gerenciados listadas aqui.

- `AWSManagedDomainsAmazonGuardDutyThreatList`— Domínios associados às descobertas de segurança do Amazon GuardDuty DNS. Os domínios são provenientes apenas dos sistemas de inteligência GuardDuty de ameaças da empresa e não contêm domínios provenientes de fontes externas de terceiros. Para obter mais informações sobre a fonte à qual o domínio na descoberta está relacionado, consulte ThreatIntelligenceDetalhes na referência da GuardDuty API. Somente domínios `ThreatIntelligenceDetail` que contenham “Amazon” na descoberta são incluídos nas Listas de Domínios AWS Gerenciados.

  Para obter mais informações sobre inteligência de ameaças de parceiros terceirizados, consulte Amazon GuardDuty Partners.

AWS As listas de domínios gerenciados não podem ser baixadas nem pesquisadas. Para proteger a propriedade intelectual, você não pode visualizar nem editar as especificações de domínio individuais em uma lista de domínios AWS gerenciados. Essa restrição também ajuda a impedir que usuários mal-intencionados criem ameaças que contornem especificamente as regras publicadas.

Para testar as listas de domínios gerenciados

Fornecemos o seguinte conjunto de domínios para testar as listas de domínios gerenciados:

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 AWSManagedDomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

Esses domínios serão resolvidos para 1.2.3.4 se eles não estiverem bloqueados. Se você estiver usando as listas de domínios gerenciados em uma VPC, a consulta desses domínios retornará a resposta para a qual uma ação de bloqueio na regra está definida (por exemplo, NODATA).

Para obter mais informações sobre listas de domínios gerenciados, entre em contato com a AWS Support Center.

A tabela a seguir lista a disponibilidade da região para listas de domínios AWS gerenciados.

Disponibilidade da região da lista de domínios gerenciado

Região	Listas de domínios gerenciados disponíveis?
Ásia-Pacífico (Mumbai)	Sim
Ásia-Pacífico (Seul)	Sim
Ásia-Pacífico (Singapura)	Sim
Ásia-Pacífico (Sydney)	Sim
Ásia-Pacífico (Tóquio)	Sim
Região Ásia-Pacífico (Osaka)	Sim
Ásia-Pacífico (Jacarta)	Sim
Ásia-Pacífico (Hyderabad)	Sim
Ásia-Pacífico (Melbourne)	Sim
Ásia-Pacífico (Hong Kong)	Sim
Região Canadá (Central)	Sim

Região	Listas de domínios gerenciados disponíveis?
Oeste do Canadá (Calgary)	Sim
Região Europa (Frankfurt)	Sim
Região Europa (Irlanda)	Sim
Região Europa (Londres)	Sim
Europa (Milão)	Sim
Região Europa (Paris)	Sim
Europa (Estocolmo)	Sim
Europa (Zurique)	Sim
Europa (Espanha)	Sim
América do Sul (São Paulo)	Sim
Leste dos EUA (Norte da Virgínia)	Sim
Leste dos EUA (Ohio)	Sim
Oeste dos EUA (N. da Califórnia)	Sim
Oeste dos EUA (Oregon)	Sim

Região	Listas de domínios gerenciados disponíveis?
África (Cidade do Cabo)	Sim
China (Pequim)	Sim
China (Ningxia)	Sim
AWS GovCloud (US)	Sim
Oriente Médio (Barém)	Sim
Oriente Médio (Emirados Árabes Unidos)	Sim
Israel (Tel Aviv)	Sim

Considerações adicionais sobre segurança

AWS As listas de domínios gerenciados foram projetadas para ajudar a protegê-lo contra ameaças comuns na Web. Quando usadas de acordo com a documentação, essas listas adicionam outra camada de segurança para as aplicações. Porém, as listas de domínios gerenciados não se destinam a substituir outros controles de segurança, que são determinadas pelos recursos da AWS que você seleciona. Para garantir que seus recursos AWS estejam protegidos adequadamente, consulte a orientação no Modelo de Responsabilidade Compartilhada.

Como atenuar cenários falsos positivos

Se você estiver encontrando cenários falsos positivos em regras que usam Listas de domínios gerenciados pela para bloquear consultas, execute as seguintes etapas:

1. Nos logs do Resolver, identifique o grupo de regras e a lista de domínios gerenciados que estão causando o falso positivo. Faça isso localizando o log para a consulta que o Firewall DNS está bloqueando, mas que você deseja permitir. O registro do log lista o grupo de regras, a ação

da regra e a lista de domínios gerenciados. Para obter mais informações sobre logs, consulte (Valores que aparecem em logs de consultas do Resolver).

2. Crie uma nova regra no grupo de regras que permita explicitamente a consulta bloqueada. Ao criar a regra, você pode definir sua própria lista de domínios apenas com a especificação de domínio que deseja permitir. Siga as orientações para o gerenciamento de regras e grupo de regras em Criar um grupo de regras e regras.
3. Priorize a nova regra dentro do grupo de regras para que ela seja executada antes da regra que está usando a lista gerenciada. Para fazer isso, dê à nova regra uma configuração de prioridade numérica mais baixa.

Quando tiver atualizado o grupo de regras, a nova regra permitirá explicitamente o nome de domínio que pretende permitir antes da execução da regra de bloqueio.

Como gerenciar suas próprias listas de domínios

Você pode criar suas próprias listas de domínios para especificar categorias de domínio que você não encontra nas ofertas de lista de domínios gerenciados ou que você mesmo prefere manipular.

Além dos procedimentos descritos nesta seção, no console, você pode criar uma lista de domínios no contexto do gerenciamento de regras do Firewall DNS do Route 53 Resolver, ao criar ou atualizar uma regra.

Cada especificação de domínio na lista de domínios deve atender aos seguintes requisitos:

- Ela pode, opcionalmente, começar com * (asterisco).
- Com exceção do asterisco inicial opcional e um ponto, como delimitador entre rótulos, ele deve conter apenas os seguintes caracteres: `A-Z`, `a-z`, `0-9`, `-` (hífen).
- Deve ter de 1 a 255 caracteres.

Quando você faz alterações em entidades do Firewall DNS, como regras e listas de domínios, o Firewall DNS propaga as alterações em todos os lugares em que as entidades são armazenadas e usadas. Suas alterações são aplicadas em segundos, mas pode haver um breve período de inconsistência quando as alterações chegam em alguns lugares e não em outros. Assim, por exemplo, se você adicionar um domínio a uma lista de domínios referenciada por uma regra de bloqueio, o novo domínio poderá ser brevemente bloqueado em uma área da VPC, enquanto ainda é permitido em outra. Essa inconsistência temporária pode ocorrer quando você configura pela

primeira vez suas associações de grupo de regras e VPC e quando você altera as configurações existentes. Geralmente, quaisquer inconsistências deste tipo duram apenas alguns segundos.

Teste sua lista de domínios antes de usá-la em produção

Como prática recomendada, antes de usar uma lista de domínios na produção, teste-a em um ambiente que não seja de produção, com a ação da regra definida como `Alert`. Avalie a regra usando CloudWatch as métricas da Amazon e os registros do Resolver. Os logs fornecem o nome da lista de domínios para todos os alertas e ações de bloqueio. Quando você estiver satisfeito de que a lista de domínios está correspondendo às consultas de DNS da maneira que você deseja, altere a configuração de ação da regra, conforme necessário. Para obter informações sobre CloudWatch métricas e registros de consultaMonitorando grupos de regras do firewall DNS do Route 53 Resolver com a Amazon CloudWatch, consulteValores que aparecem em logs de consultas do Resolver, Como gerenciar configurações de log de consultas do Resolver e.

Para adicionar uma lista de domínios

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC. Continue na etapa 2.

   - OU -

   Faça login no AWS Management Console e abra o

   o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em DNS Firewall, escolha Listas de domínios. Na página Domain lists (Listas de domínios) você pode selecionar e editar listas de domínios existentes e adicionar suas próprias.
3. Para adicionar uma lista de domínios, selecione Add domain list (Adicionar lista de domínios).
4. Forneça um nome para sua lista de domínios e insira suas especificações de domínio na caixa de texto, um por linha.

   Se você deslizar a opção Switch to bulk upload (Alternar para carga em massa) para on (ativado), insira o URI do bucket do Amazon S3 onde você criou uma lista de domínios. Esta lista de domínios deve ter um nome de domínio por linha.

> **Note**
>
> Nomes de domínio duplicados farão com que a importação em massa falhe.

5. Escolha Add domain list (Adicionar lista de domínios). A página Domain lists (Listas de domínios) lista sua nova lista de domínios.

Depois de criar a lista de domínios, pode referenciá-la por nome a partir das regras do Firewall DNS.

Como excluir entidades do Firewall DNS

Quando você exclui uma entidade que pode usar no Firewall DNS, como uma lista de domínios que pode estar em uso em um grupo de regras ou um grupo de regras que possa estar associado a uma VPC, o Firewall DNS verifica se a entidade está sendo usada no momento. Se ele descobrir que ela está sendo usada, o Firewall DNS avisa. O Firewall DNS quase sempre é capaz de determinar se uma entidade está sendo usada. No entanto, em casos raros, talvez não seja possível fazer isso. Se você precisar ter certeza de que nada está usando a entidade no momento, verifique nas configurações do Firewall DNS antes de excluí-lo. Se a entidade for uma lista de domínios referenciada, verifique se nenhum grupo de regras está utilizando-a. Se a entidade for um grupo de regras, verifique se ela não está associada a nenhuma VPC.

Para excluir uma lista de domínios

1. No painel de navegação, escolha Domain lists (Listas de domínios).
2. Na barra de navegação, escolha a região da lista de domínios.
3. Selecione a lista de domínios que você deseja excluir e escolha Delete (Excluir) e confirme a exclusão.

Configurar o registro para Firewall DNS

Você pode avaliar suas regras de firewall de DNS usando as CloudWatch métricas da Amazon e os registros de consulta do Resolver. Os logs fornecem o nome da lista de domínios para todos os alertas e ações de bloqueio. Para obter mais informações sobre a Amazon CloudWatch, consulteMonitorando grupos de regras do firewall DNS do Route 53 Resolver com a Amazon CloudWatch.

Quando você habilitar o Firewall DNS, associe-o a uma VPC à qual habilitou o registro, `firewall_rule_group_id` , `firewall_rule_action` e `firewall_domain_list_id` são os campos específicos do Firewall DNS fornecidos em seus logs.

> **Note**
>
> Os logs de consultas mostrarão campos adicionais do DNS Firewall somente para as consultas bloqueadas pelas regras do DNS Firewall.

Para iniciar o registro das consultas de DNS que são filtradas pelas regras do Firewall DNS originadas em suas VPCs, execute as seguintes tarefas no console do Amazon Route 53:

Para configurar o log de consulta do Resolver para o DNS Firewall

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Expanda o menu do console do Route 53. No canto superior esquerdo do console, escolha o ícone de três barras horizontais ().
3. No menu Resolver, escolha Query logging (Log de consultas).
4. No seletor de região, escolha a AWS região em que você deseja criar a configuração de registro de consultas.

   Essa deve ser a mesma região onde você criou as VPCs associadas ao Firewall DNS para as quais você deseja registrar consultas. Se você tiver VPCs em várias regiões, deverá criar pelo menos uma configuração do log de consultas para cada região.
5. Escolha Configure query logging (Configurar log de consultas).
6. Especifique os seguintes valores:

   Nome da configuração do log de consultas

   Insira um nome para sua configuração do log de consultas. O nome é exibido no console na lista de configurações do log de consultas. Insira um nome que o ajudará a encontrar essa configuração posteriormente.

Destino dos logs de consulta

Escolha o tipo de AWS recurso para o qual você deseja que o Resolver envie registros de consulta. Para obter informações sobre como escolher entre as opções (grupo de CloudWatch registros de registros, bucket do S3 e stream de entrega do Firehose), consulte. AWS recursos para os quais você pode enviar registros de consulta do Resolver

Depois de escolher o tipo de recurso, você pode criar outro recurso desse tipo ou escolher um recurso existente criado pela AWS conta atual.

> **Note**
>
> Você pode escolher somente recursos criados na caixa de diálogo região da AWS escolhida na etapa 4, a região onde você está criando a configuração de log de consultas. Se você optar por criar um novo recurso, esse recurso será criado na mesma região.

VPCs para as quais registrar consultas em log

Essa configuração de log de consultas registrará consultas de DNS originadas nas VPCs que você escolher. Marque a caixa de seleção de cada VPC na região atual para a qual deseja que o Resolver registre consultas e escolha Choose (Escolher).

> **Note**
>
> A entrega de log da VPC pode ser habilitada apenas uma vez para um tipo de destino específico. Os logs não podem ser entregues a vários destinos do mesmo tipo. Por exemplo, os logs da VPC não podem ser entregues a dois destinos do Amazon S3.

7. Escolha Configure query logging (Configurar log de consultas).

> **Note**
>
> Você deve começar a ver consultas de DNS feitas por recursos em sua VPC nos logs em alguns minutos após a criação bem-sucedida da configuração do log de consultas.

Compartilhando grupos de regras do Route 53 Resolver DNS Firewall entre contas AWS

Você pode compartilhar grupos de regras do DNS Firewall entre AWS contas. Para compartilhar grupos de regras, você usa AWS Resource Access Manager (AWS RAM). O console do DNS Firewall se integra ao AWS RAM console. Para obter mais informações sobre AWS RAM, consulte o Guia do Usuário do Resource Access Manager.

Observe o seguinte:

Associação de grupos de regras compartilhadas com VPCs

Se outra AWS conta tiver compartilhado um grupo de regras com sua conta, você poderá associá-lo às suas VPCs da mesma forma que associa os grupos de regras que você criou. Para ter mais informações, consulte Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver.

Exclusão ou interrupção do compartilhamento de um grupo de regras

Se você compartilhar um grupo de regras com outras contas e, em seguida, excluir o grupo de regras ou parar de compartilhá-lo, o DNS Firewall removerá todas as associações criadas pelas outras contas entre o grupo de regras e suas VPCs.

Configurações máximas para grupos de regras e associações

Grupos de regras compartilhadas e suas associações com VPCs são incluídos nas contagens das contas com as quais os grupos de regras são compartilhados.

Para as cotas do Firewall DNS atuais, consulte Cotas no Firewall de DNS do Route 53 Resolver.

Permissões

Para compartilhar um grupo de regras com outra AWS conta, você deve ter permissão para usar a ação PutFirewallRuleGroupPolítica.

Restrições na AWS conta com a qual um grupo de regras é compartilhado

A conta com a qual um grupo de regras é compartilhado não pode alterar ou excluir o grupo de regras.

Tags

Somente a conta que criou um grupo de regras pode adicionar, excluir ou consultar tags no grupo de regras.

Para visualizar o status de compartilhamento atual de um grupo de regras (incluindo a conta que compartilhou o grupo de regras ou a conta com a qual um grupo de regras é compartilhado) e para compartilhar grupos de regras com outra conta, realize o procedimento a seguir.

Para ver o status de compartilhamento e compartilhar grupos de regras com outra AWS conta

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Grupos de regras.
3. Na barra de navegação, escolha a região onde o grupo de regras foi criado.

   A coluna Sharing status (Status de compartilhamento) mostra o status de compartilhamento atual dos grupos de regras criados pela conta atual ou que foram compartilhados com a conta atual:

   - Não compartilhado: a AWS conta atual criou o grupo de regras e o grupo de regras não é compartilhado com nenhuma outra conta.
   - Shared by me (Compartilhada por mim): a conta atual criou o grupo de regras e compartilhou com uma ou mais contas.
   - Shared with me (Compartilhada comigo): outra conta de criou o grupo de regras e o compartilhou com a conta atual.
4. Escolha o nome do grupo de regras para o qual você deseja exibir informações de compartilhamento ou deseja compartilhar com outra conta.

   Na página Rule group: ***rule group name*** (Grupo de regras: nome do grupo de regras), o valor em Owner (Proprietário) exibe o ID da conta que criou o grupo de regras. Essa é a conta atual, a menos que o valor do Sharing status (Status de compartilhamento) seja Shared with me (Compartilhada comigo). Neste caso, Owner (Proprietário) é a conta que criou o grupo de regras e compartilhou com a conta atual.
5. Escolha Share (Compartilhar) para visualizar informações adicionais ou para compartilhar o grupo de regras com outra conta. Uma página no AWS RAM console é exibida, dependendo do valor do status de compartilhamento:

   - Não compartilhada: a página Create resource share (Criar compartilhamento de recurso) é exibida. Para obter informações sobre como compartilhar o grupo de regras com outra conta, unidade organizacional (OU) ou organização, vá para a etapa que se segue a essa.

- Shared by me (Compartilhada por mim): a página Shared resources (Recursos compartilhados) mostra os grupos de regras e outros recursos de propriedade da conta atual e compartilhados com outras contas.
- Shared with me (Compartilhada comigo): a página Shared resources (Recursos compartilhados) mostra os grupos de regras e outros recursos de propriedade de outras contas e compartilhados com a conta atual.

6. Para compartilhar um grupo de regras com outra AWS conta, OU ou organização, especifique os valores a seguir.

> **Note**
>
> Não é possível atualizar as configurações de compartilhamento. Se quiser alterar qualquer uma das configurações a seguir, é necessário compartilhar um grupo de regras novamente com as novas configurações e, em seguida, remover as configurações de compartilhamento antigas.

Descrição

Insira uma breve descrição que ajude a lembrar o motivo do compartilhamento do grupo de regras.

Recursos

Marque a caixa de seleção do grupo de regras que deseja compartilhar.

Entidades principais

Insira o número da AWS conta, o nome da OU ou o nome da organização.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Essas são as tags que AWS Billing and Cost Management permitem organizar sua AWS fatura; você também pode usar tags para outros fins. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing .

Como habilitar as proteções do Firewall DNS do Route 53 Resolver para a VPC

Você habilita as proteções do Firewall DNS para sua VPC associando um ou mais grupos de regras à VPC. Sempre que uma VPC é associada a um grupo de regras do Firewall DNS, o Route 53 Resolver fornece as seguintes proteções do Firewall DNS:

- O Resolver encaminha as consultas de DNS de saída da VPC através do Firewall DNS e o Firewall DNS filtra as consultas usando os grupos de regras associados.
- O Resolver impõe as configurações na configuração do Firewall DNS da VPC.

Para fornecer proteções de DNS Firewall à sua VPC, faça o seguinte:

- Crie e gerencie associações entre seus grupos de regras do Firewall DNS e sua VPC. Para obter informações sobre grupos de regras, consulte Regras e grupos de regras do Firewall DNS.
- Configure como deseja que o Resolver manipule consultas de DNS para a VPC durante uma falha, por exemplo, se o Firewall DNS não fornecer uma resposta para uma consulta de DNS.

Como gerenciar associações entre a VPC e o grupo de regras do Firewall DNS do Route 53 Resolver

Para exibir as associações de VPC de um grupo de regras

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   Escolha Firewall do DNS no painel de navegação para abrir a página Grupos de regras do firewall do DNS no console do Amazon VPC.

   - OU -

   Faça login no AWS Management Console e abra o

   o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em Firewall do DNS, escolha Grupos de regras.
3. Na barra de navegação, escolha a região do grupo de regras.

4. Selecione o grupo de regras que você deseja associar.
5. Escolha Exibir detalhes. A página do grupo de regras será exibida.
6. Na parte inferior, você pode ver uma área de detalhes com guias que inclui regras e VPCs associadas. Escolha a guia Associated VPCs (VPCs associadas).

Para associar um grupo de regras a uma VPC

1. Localize as associações de VPC do grupo de regras seguindo as instruções no procedimento anterior para exibir as associações de VPC de um grupo de regras.
2. Na guia Associated VPCs, escolha Associate VPC (Associar VPC).
3. Localize a VPC que você deseja associar ao grupo de regras no menu suspenso. Selecione-a e escolha Associate (Associar).

Na página do grupo de regras, sua VPC está listada na guia Associated VPCs (VPCs associadas). Em primeiro lugar, Status reporta Updating (Atualizando). Quando a associação for concluída, o status será alterado para Complete (Concluído).

Para remover uma associação entre um grupo de regras e uma VPC

1. Localize as associações de VPC do grupo de regras seguindo as instruções no procedimento anterior para exibir as associações de VPC de um grupo de regras.
2. Selecione a VPC que você deseja remover da lista e escolha Disassociate (Desassociar). Verifique e confirme a ação.

Na página do grupo de regras, sua VPC está listada na guia Associated VPCs com o status Disassociating (Desassociando). Quando a operação for concluída, o Firewall DNS atualizará a lista para remover a VPC.

Configuração da VPC do Firewall DNS

A configuração do DNS Firewall para a VPC determina se o Route 53 Resolver deixa passar ou bloqueia consultas durante as falhas, por exemplo, quando o DNS Firewall está inoperante, não responde ou não está disponível naquela zona. O Resolver impõe a configuração de firewall de uma VPC sempre que você tiver um ou mais grupos de regras de Firewall DNS associados à VPC.

Você pode configurar uma VPC para não abrir ou fechar.

- Por padrão, o modo de falha é fechado, o que significa que o Resolver bloqueia todas as consultas para as quais não recebe uma resposta do DNS Firewall e envia uma resposta de `SERVFAIL` do DNS. Essa abordagem favorece a segurança, em vez da disponibilidade.
- Se você habilitar para não abrir, o Resolver permitirá consultas, se ele não receber uma resposta do Firewall DNS. Essa abordagem favorece a disponibilidade, em vez da segurança.

Para alterar a configuração do Firewall DNS para uma VPC (console)

1. Faça login AWS Management Console e abra o console do Resolver em https://console.aws.amazon.com/route53resolver/.
2. No painel de navegação, em Resolvers, escolha VPCs.
3. Na página VPCs, localize e edite a VPC. Altere a configuração do Firewall DNS para não abrir ou fechar, conforme necessário.

Para alterar o comportamento do Firewall DNS para uma VPC (API)

- Atualize a configuração do firewall da VPC chamando UpdateFirewallConfig e ativando ou desativando. `FirewallFailOpen`

Você pode recuperar uma lista das configurações de firewall da VPC por meio da API chamando Configs. ListFirewall

Perfis do Amazon Route 53

Com os Perfis do Route 53, você pode aplicar e gerenciar configurações do Route 53 relacionadas ao DNS em várias VPCs e em diferentes. Contas da AWS Os perfis tornam o gerenciamento das configurações de DNS para muitas VPCs tão fácil quanto gerenciá-las para uma única VPC. Quando você atualiza um perfil, suas configurações são propagadas para todas as VPCs associadas ao perfil. Você também pode compartilhar um perfil com Contas da AWS as mesmas regiões usando AWS RAM. Os recursos atualmente compatíveis com o Route 53 que você pode associar a um perfil são:

- Zonas hospedadas privadas e as configurações especificadas nelas.
- Regras do Route 53 Resolver, tanto de encaminhamento quanto de sistema.
- Grupos de regras do DNS Firewall.

Algumas das configurações de VPC são gerenciadas diretamente no perfil. As configurações são:

- Configuração de pesquisa reversa de DNS para regras de resolução.
- Configuração do modo de falha do firewall DNS.
- Configuração de validação do DNSSEC.

Por exemplo, você pode ativar a configuração do modo de falha do firewall DNS para todas as VPCs às quais o perfil está associado, mas manter a configuração de validação de DNSSEC existente da VPC.

Você também pode usar AWS CloudFormation para definir configurações de DNS consistentes para VPCs recém-provisionadas.

Você pode associar um perfil por VPC e o número de recursos que você pode associar por perfil varia. Para ter mais informações, consulte Cotas nos perfis do Route 53 .

Como as configurações do perfil do Route 53 são priorizadas

Você pode definir as configurações e associações de DNS locais para Perfis para migração ou outros fins de teste. Quando uma consulta de DNS corresponde à regra Resolver para uma zona hospedada privada diretamente associada à VPC e à regra Resolver para uma zona hospedada privada associada ao Perfil, as configurações de DNS locais têm precedência. Quando uma consulta

de DNS é feita para um nome de domínio conflitante, o mais específico ganha. A tabela a seguir inclui exemplos da ordem de avaliação:

consulta ao DNS	Regra de perfil	Regra de VPC	Regra avaliada
exemplo.com	exemplo.com	exemplo.com	VPC local
test.example.com	test.example.com	exemplo.com	Perfil
marketing.example.com	Nenhum	marketing.example.com	VPC local

Disponibilidade da região de perfis do Route 53

Os perfis do Route 53 estão disponíveis na maioria dos perfis comerciais Regiões da AWS. A tabela a seguir fornece uma lista da disponibilidade atual.

Disponibilidade da região de perfis do Route 53

Região	Perfis disponíveis?
África (Cidade do Cabo)	Sim
Ásia-Pacífico (Hong Kong)	Sim
Ásia-Pacífico (Hyderabad)	Sim
Ásia-Pacífico (Jacarta)	Sim
Ásia-Pacífico (Melbourne)	Sim
Ásia-Pacífico (Mumbai)	Sim
Região Ásia-Pacífico (Osaka)	Sim
Região Ásia-Pacífico (Seul)	Sim
Ásia-Pacífico (Singapura)	Sim

Região	Perfis disponíveis?
Ásia-Pacífico (Sydney)	Sim
Região Ásia-Pacífico (Tóquio)	Sim
Canadá (Central)	Sim
Oeste do Canadá (Calgary)	Sim
Região Europa (Frankfurt)	Sim
Região Europa (Irlanda)	Sim
Europa (Londres)	Sim
Europa (Milão)	Sim
Europa (Paris)	Sim
Europa (Espanha)	Sim
Europa (Estocolmo)	Sim
Europa (Zurique)	Sim
Israel (Tel Aviv)	Sim
Oriente Médio (Barém)	Sim
Oriente Médio (Emirados Árabes Unidos)	Sim
América do Sul (São Paulo)	Sim
Leste dos EUA (Ohio)	Sim
Oeste dos EUA (Oregon)	Sim
Oeste dos EUA (N. da Califórnia)	Sim
Leste dos EUA (Norte da Virgínia)	Sim

Etapas de alto nível para usar perfis do Route 53

Para implementar os perfis do Amazon Route 53 em suas VPCs da Amazon Virtual Private Cloud, você executa as seguintes etapas de alto nível.

1. Criar um perfil vazio — A primeira etapa é criar um perfil vazio ao qual você possa associar recursos de DNS. Para ter mais informações, consulte Criação de perfis do Route 53.
2. Associar recursos DNS ao perfil — Os recursos que você pode associar atualmente a um perfil são zonas hospedadas privadas, regras do Route 53 Resolver, tanto de encaminhamento quanto de sistema, e grupos de regras de firewall DNS. Para obter mais informações, consulteAssociar grupos de regras do DNS Firewall a um perfil do Route 53,Associar zonas hospedadas privadas a um perfil do Route 53,Associe as regras do Resolver a um perfil do Route 53.
3. Defina algumas das configurações de VPC para o perfil — Algumas das configurações de DNS, como zonas hospedadas associadas ao perfil, são aplicadas às VPCs imediatamente. Para a validação do DNSSEC, a pesquisa reversa de DNS do Resolver e as configurações do modo de falha do Firewall do DNS, você pode escolher uma das seguintes opções:
   - Para a validação do DNSSEC, você pode optar por usar a configuração local da VPC (padrão), ativar a validação ou desabilitar a validação para todas as VPCs associadas ao perfil.
   - Para a configuração de pesquisa reversa de DNS do Resolver, você pode ativá-la, desativá-la ou usar as regras definidas automaticamente para a VPC localmente (padrão).
   - Para a configuração do modo de falha do Firewall DNS, você pode ativá-lo, desativá-lo ou usar a configuração do modo de falha definida para a VPC localmente (padrão).

   Para ter mais informações, consulte Editar configurações do perfil do Route 53.
4. Associe o perfil a uma ou mais VPCs — Para começar a usar seu perfil, associe-o a uma ou mais VPCs. Para ter mais informações, consulte Associar um perfil do Route 53 às VPCs.

Criação de perfis do Route 53

Para criar perfis do Route 53, siga as orientações neste tópico. Escolha uma guia para criar um perfil do Route 53 usando o console do Route 53 ou AWS CLI.

- Console
- CLI

Console

Para criar um perfil do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Na barra de navegação, escolha a região em que você deseja criar o perfil.
4. Insira um nome para o Perfil, opcionalmente adicione tags e escolha Criar Perfil.

   Isso cria um Perfil vazio com configurações padrão às quais você pode associar recursos. Depois de associar recursos ao Perfil, você pode associá-lo a várias VPCs e editar a forma como algumas das configurações do Resolver se aplicam às VPCs.

CLI

Você pode criar um perfil executando um AWS CLI comando como o seguinte e usando seu próprio valor para`name`.

```
aws route53profiles create-profile --name test
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
}
```

Para associar seus perfis a diferentes recursos e editar as configurações de VPC para o perfil, consulte os procedimentos a seguir:

Tópicos

Associar grupos de regras do DNS Firewall a um perfil do Route 53

Escolha uma guia para associar grupos de regras do Firewall DNS a um perfil do Route 53 usando o console do Route 53 ou AWS CLI.

- Console
- CLI

Console

Para associar grupos de regras do Firewall DNS

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na barra de navegação, escolha a região em que você criou o perfil.
3. No painel de navegação, escolha Perfis e, na tabela Perfis, escolha o nome vinculado do Perfil com o qual você deseja trabalhar.
4. Na <Profile name>página, escolha a guia Grupos de regras do Firewall DNS e, em seguida, Associar.
5. Na seção Grupos de regras do Firewall DNS, você pode selecionar até 10 grupos de regras que você criou anteriormente. Se você quiser associar mais de 10 grupos de regras, use as APIs. Para obter mais informações, consulte AssociateResourceToProfile.

   Para criar novos grupos de regras, consulteCriar um grupo de regras e regras.
6. Selecione Next (Próximo).

7. Na página Definir prioridade, você pode definir a ordem na qual os grupos de regras são processados clicando no número de prioridade pré-atribuído e digitando um novo. Os valores permitidos para a prioridade estão entre 100 e 9900.

   Os grupos de regras são avaliados começando com a configuração de prioridade numérica mais baixa e subindo. Você pode alterar a prioridade de um grupo de regras a qualquer momento, por exemplo, para alterar a ordem do processamento ou abrir espaço para outros grupos de regras.

   Selecione Enviar.
8. O progresso da associação é exibido na coluna Status na caixa de diálogo de grupos de regras do Firewall DNS.

CLI

Você pode associar um grupo de regras a um perfil executando um AWS CLI comando como o seguinte e usando seus próprios valores para `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}"
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
```

```
}
```

Associar zonas hospedadas privadas a um perfil do Route 53

Siga as etapas deste procedimento para associar uma zona hospedada privada a um perfil.

Para associar zonas hospedadas privadas

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na barra de navegação, escolha a região em que você criou o perfil.
3. No painel de navegação, escolha Perfis e, na tabela Perfis, escolha o nome vinculado do Perfil com o qual você deseja trabalhar.
4. Na <Profile name>página, escolha a guia Zonas hospedadas privadas e, em seguida, Associar.
5. Na página Associar zonas hospedadas privadas, você pode selecionar até 10 zonas hospedadas privadas que você criou anteriormente. Se você quiser associar mais de 10 zonas hospedadas privadas, use as APIs. Para obter mais informações, consulte AssociateResourceToProfile.

   Para criar zonas hospedadas privadas, consulteCriar uma zona hospedada privada.
6. Escolha Associado
7. O progresso da associação é exibido na coluna Status na página Zonas hospedadas privadas.

Associe as regras do Resolver a um perfil do Route 53

Siga as etapas deste procedimento para associar as regras do Resolver a um perfil.

Para associar as regras do Resolver

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na barra de navegação, escolha a região em que você criou o perfil.
3. Na <Profile name>página, escolha a guia Regras do Resolver e, em seguida, Associar.
4. Na página Associate Resolver rules, na tabela de regras do Resolver, você pode selecionar até 10 regras do Resolver que você criou anteriormente. Se você quiser associar mais de 10 regras de resolução, use as APIs. Para obter mais informações, consulte AssociateResourceToProfile.

Para criar regras do Resolver, consulteCriar regras de encaminhamento.

5. Escolha Associado
6. O progresso da associação é exibido na coluna Status na página de regras do Resolver.

Editar configurações do perfil do Route 53

Depois de associar recursos a um perfil, você pode editar as configurações padrão da VPC para decidir como elas são aplicadas às VPCs.

Para editar as configurações do perfil

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na barra de navegação, escolha a região em que você criou o perfil.
3. No painel de navegação, escolha Perfis e, na tabela Perfis, escolha o nome vinculado do Perfil com o qual você deseja trabalhar.
4. Na <Profile name>página, escolha a guia Configuração e, em seguida, Editar.
5. Na página Editar configuração, escolha um dos valores para a configuração do VPC DNSSEC, a configuração de pesquisa reversa de DNS do Resolver e a configuração do modo de falha do firewall DNS.

   Para obter mais informações sobre os valores, consulteConfigurações para o perfil do Route 53.
6. Selecione Atualizar.

Configurações para o perfil do Route 53

Ao editar uma configuração de perfil do Route 53, você especifica os seguintes valores:

Configuração do DNSSEC

Escolha um dos seguintes valores:

- Use a configuração local do VPC DNSSEC - padrão

  Escolha essa opção para que todas as VPCs associadas a esse perfil mantenham sua configuração local de validação do DNSSEC.

- Ativar a validação do DNSSEC

  Escolha essa opção para ativar a validação do DNSSEC em todas as VPCs associadas a esse perfil.

- Desativar a validação do DNSSEC

  Escolha essa opção para desativar a validação do DNSSEC em todas as VPCs associadas a esse perfil.

Configuração de pesquisa reversa de DNS do resolvedor

Escolha um dos seguintes valores:

- Habilitar

  Escolha essa opção para criar regras definidas automaticamente para pesquisa reversa de DNS em todas as VPCs associadas.

- Não habilitado

  Escolha essa opção para não criar regras definidas automaticamente para pesquisa reversa de DNS em todas as VPCs associadas.

- Use regras locais definidas automaticamente - padrão

  Escolha essa opção para usar as configurações de VPC locais para pesquisa reversa de DNS para as VPCs associadas.

Configuração do modo de falha do firewall DNS

Escolha um dos seguintes valores:

- Desabilitar

  Escolha essa opção para fechar o modo de falha do Firewall DNS para as VPCs associadas. Com essa opção, o DNS Firewall bloqueará todas as consultas que não puder avaliar adequadamente.

- Ativado

  Escolha essa opção para manter o modo de falha do Firewall DNS aberto para todas as VPCs associadas. Com essa opção, o DNS Firewall permitirá que as consultas continuem se não for possível avaliá-las adequadamente.

- Use as configurações do modo de falha local - padrão

Escolha essa opção para usar as configurações locais do modo de falha do VPC DNS Firewall.

Para obter mais informações sobre as configurações, consulte

- Como habilitar validação de DNSSEC no Amazon Route 53
- Regras de encaminhamento para consultas DNS reversas no Resolver
- Configuração da VPC do Firewall DNS

Associar um perfil do Route 53 às VPCs

Para associar um perfil do Route 53 a uma VPC, siga as orientações neste tópico. Escolha uma guia para associar um perfil do Route 53 a uma VPC usando o console do Route 53 ou. AWS CLI

- Console
- CLI

Console

Para associar VPCs

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na barra de navegação, escolha a região em que você criou o perfil.
3. Na <Profile name>página, escolha a guia VPCs e, em seguida, Associar.
4. Na página Associate VPCs, você pode selecionar até 10 VPCs que você criou anteriormente. Se você quiser associar mais de 10 VPCs, use as APIs. Para obter mais informações, consulte AssociateProfile.
5. Escolha Associado
6. O progresso da associação é exibido na coluna Status na página VPCs.

CLI

Você pode listar os perfis executando um AWS CLI comando como o seguinte e usando seus próprios valores para `nameprofile-id`, `eresource-id`:

```
aws route53profiles associate-profile --name test-association --profile-
id rp-4987774726example --resource-id vpc-0af3b96b3example
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
}
```

Visualização e atualização de perfis do Amazon Route 53

Escolha a guia do console para visualizar e editar o perfil do Route 53. Escolha a guia CLI a ser usada AWS CLI para listar os perfis que você possui, são compartilhados por você ou compartilhados com você.

- Console
- CLI

Console

Visualizando e atualizando perfis do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.

3. Selecione o botão ao lado do nome do Perfil que você deseja visualizar ou editar.
4. Na <Profile name>página, você pode visualizar os recursos DNS atualmente associados, associar novos e editar as tags e as configurações de VPC.

CLI

Você pode listar os perfis executando um AWS CLI comando como o seguinte:

```
aws route53profiles list-profiles
```

Veja a seguir um exemplo de saída depois de executar o comando:

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

Você pode obter informações sobre um determinado VPS ao qual o Perfil está associado executando um AWS CLI comando como o seguinte e usando seu próprio valor para`profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }   ]
}
```

Excluindo um perfil do Amazon Route 53

Escolha uma guia para excluir um perfil do Route 53 usando o console do Route 53 ou AWS CLI.

- Console
- CLI

Console

Para excluir um perfil do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Selecione o botão ao lado do nome do Perfil que você deseja excluir e escolha Excluir.

> **Important**
>
> Você não pode excluir um perfil se ele estiver associado a VPCs. Além disso, se o perfil for compartilhado com outro Conta da AWS, todas as VPCs às quais as configurações do perfil estejam associadas perderão essas configurações.

4. Na <Profile name>caixa de diálogo Excluir**`confirm`**, digite e escolha Excluir.

CLI

> **Important**
>
> Você não pode excluir um perfil se ele estiver associado a VPCs. Além disso, se o perfil for compartilhado com outro Conta da AWS, todas as VPCs às quais as configurações do perfil estejam associadas perderão essas configurações.

Você pode excluir um perfil executando um AWS CLI comando como o seguinte e usando seu próprio valor para`profile-id`:

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
}
```

Visualizando e atualizando recursos do Route 53 associados a um perfil do Amazon Route 53

Escolha a guia do console para visualizar as associações de recursos do perfil do Route 53 e, opcionalmente, edite a prioridade do grupo de regras do DNS Firewall. Escolha a guia CLI a ser usada AWS CLI para listar as associações de recursos e ver um exemplo de atualização para uma prioridade de um grupo de regras do Firewall DNS.

- Console
- CLI

Console

Para visualizar e atualizar recursos associados a um perfil

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Na barra de navegação, escolha a região em que você criou o perfil.
4. Selecione o botão ao lado do nome do Perfil para o qual você deseja visualizar ou editar as associações de recursos.
5. Na <Profile name>página, escolha a guia do recurso que você deseja visualizar ou editar, seja grupos de regras do Firewall DNS, Zonas hospedadas privadas ou regras do Resolvedor.
6. Na página de guia de um recurso, você pode ver os nomes, o ARN e o status dos recursos associados. Você também pode escolher o ícone de engrenagem para ajustar o que é exibido na tabela de recursos.

   Na página da guia Grupos de regras do Firewall DNS, você também pode escolher a entrada de prioridade do grupo de regras e editá-la para um número menor ou maior. Os grupos de regras são avaliados em ordem, começando pelo número de prioridade mais baixa até o número de maior prioridade.

CLI

Você pode listar recursos associados a um perfil executando um AWS CLI comando como o seguinte e usando seu próprio valor para`profile-id`:

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

Veja a seguir um exemplo de saída depois de executar o 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"
        }
    ]
}
```

Você pode atualizar a prioridade de um grupo de regras do DNS Firewall associado a um perfil executando um AWS CLI comando como o seguinte e usando seu próprio valor para e usando seus próprios valores para `profile-resource-association-id` e`--resource-properties`:

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
}
```

Desassociando um recurso de um perfil do Amazon Route 53

Para desassociar um recurso associado a um perfil do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Na barra de navegação, escolha a Região em que o Perfil do qual você deseja desassociar um recurso foi criado.
4. Selecione o botão ao lado do nome do Perfil do qual você deseja desassociar um recurso.
5. Na <Profile name>página, escolha a guia do recurso que você deseja excluir, seja grupos de regras do Firewall DNS, Zonas hospedadas privadas ou regras do Resolvedor.
6. Na página de guia do recurso, escolha o recurso que você deseja desassociar e, em seguida, Desassociar.
7. Na caixa de diálogo Dissociar recursos, digite e escolha Dissociar. **`confirm`**

Visualização de VPCs associadas a um perfil do Amazon Route 53

Escolha a guia do console para visualizar e editar o perfil do Route 53 para associações de VPC. Escolha a guia CLI a ser usada AWS CLI para listar o perfil para associações de VPC ou para obter informações sobre uma associação específica

- Console
- CLI

Console

Para visualizar VPCs associadas a um perfil

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Na barra de navegação, escolha a região em que você criou o perfil.
4. Selecione o botão ao lado do nome do perfil para o qual você deseja visualizar as VPCs associadas.

5. Na <Profile name>página, escolha a guia VPCs.
6. Na página da guia para VPCs, você pode ver os nomes, o ARN e o status das VPCs associadas.

CLI

Você pode listar as VPCs às quais o perfil está associado executando um AWS CLI comando como o seguinte:

```
aws route53profiles list-profile-associations
```

Veja a seguir um exemplo de saída depois de executar o 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"
        }
    ]
}
```

Você pode obter informações sobre um determinado VPS ao qual o Perfil está associado executando um AWS CLI comando como o seguinte e usando seu próprio valor para`profile-association-id`:

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }   ]
}
```

Desassociando uma VPC de um perfil do Amazon Route 53

Escolha uma guia para dissociar um perfil do Route 53 de uma VPC usando o console do Route 53 ou. AWS CLI

- Console
- CLI

Console

Para desassociar uma VPC associada a um perfil do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Na barra de navegação, escolha a região em que o perfil do qual você deseja desassociar uma VPC foi criado.

4. Selecione o botão ao lado do nome do Perfil do qual você deseja desassociar uma VPC.
5. Na <Profile name>página, escolha a guia VPCs.
6. Na página da guia VPCs do recurso, escolha a VPC que você deseja desassociar e, em seguida, Desassociar.
7. Na caixa de diálogo Dissociar recursos, digite e escolha Dissociar. **`confirm`**

CLI

Você pode dissociar um perfil de uma VPC executando um AWS CLI comando como o seguinte e usando seu próprio valor para e: `profile-id` `--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

Veja a seguir um exemplo de saída depois de executar o 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"
    }
```

Trabalhando com perfis compartilhados do Route 53

Você pode compartilhar um perfil com outras contas da seguinte forma:

- Conceder permissões somente de leitura, o que significa que a outra conta pode associar o perfil às suas VPCs. Nesse caso, todos os recursos e configurações de DNS entrarão em vigor nas VPCs associadas.
- Conceder permissões de administrador. Nesse caso, as contas com o perfil compartilhado podem modificar o perfil e depois associá-lo às suas VPCs. Um proprietário também pode criar permissões gerenciadas pelo cliente que podem ser usadas para especificar quais ações podem

ser executadas pela conta do consumidor. Para obter mais informações, consulte Permissões gerenciadas pelo cliente no Guia AWS RAM do usuário.

O perfil do Amazon Route 53 se integra com AWS Resource Access Manager (AWS RAM) para permitir o compartilhamento de recursos. AWS RAM é um serviço que permite que você compartilhe alguns recursos do Route 53 com outros Contas da AWS ou por meio deles AWS Organizations. Com AWS RAM, você compartilha recursos de sua propriedade criando um compartilhamento de recursos. Um compartilhamento de atributos especifica os atributos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem incluir:

- Específico Contas da AWS
- Uma unidade organizacional dentro de sua organização em AWS Organizations
- Toda a sua organização em AWS Organizations

Para obter mais informações sobre AWS RAM, consulte o Guia AWS RAM do usuário.

Este tópico explica como compartilhar recursos que você possui e como usar os recursos que são compartilhados com você.

Conteúdo

Pré-requisitos para compartilhar perfis do Route 53

- Para compartilhar um perfil do Route 53, você deve possuí-lo em seu Conta da AWS. Isso significa que o recurso deve ser alocado ou provisionado em sua conta. Você não pode compartilhar um perfil do Route 53 que tenha sido compartilhado com você.
- Para compartilhar um perfil do Route 53 com sua organização ou unidade organizacional em AWS Organizations, você deve habilitar o compartilhamento com AWS Organizations. Para obter mais

informações, consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM .

Compartilhando um perfil do Route 53

Ao compartilhar um Perfil que você possui com outra pessoa Conta da AWS, você permite que ela aplique as configurações relacionadas ao DNS do Perfil às suas VPCs. Isso facilita a aplicação de configurações uniformes de DNS em milhares de VPCs com o mínimo de sobrecarga de gerenciamento.

Para compartilhar um perfil do Route 53, você deve adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre Contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Ao compartilhar um perfil do Route 53 usando o console do Route 53, você o adiciona a um compartilhamento de recursos existente. Para adicionar o perfil do Route 53 a um novo compartilhamento de recursos, primeiro você deve criar o compartilhamento de recursos usando o AWS RAM console.

Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro de sua organização está ativado, os consumidores em sua organização recebem automaticamente acesso ao perfil compartilhado do Route 53. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e terão acesso ao perfil compartilhado do Route 53 após aceitarem o convite.

Você pode começar a compartilhar um perfil do Route 53 que você possui no console do Route 53 e continuar no AWS RAM console.

Para compartilhar um perfil do Route 53 que você possui usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Selecione o perfil que você deseja compartilhar e, na página de detalhes do perfil, escolha Gerenciar compartilhamento.
4. Você é direcionado ao AWS RAM console, onde pode seguir estas etapas: Criando um compartilhamento de recursos no Guia do AWS RAM usuário.
5. Se um Perfil for compartilhado com você, a tabela Perfis incluirá o texto Compartilhado comigo.

Quando você compartilha um Perfil, ele é listado como Compartilhado na tabela Perfis.

Para compartilhar um perfil do Route 53 que você possui usando o AWS RAM console

Consulte Criar um compartilhamento de atributos no Manual do usuário do AWS RAM .

Para compartilhar um perfil do Route 53 que você possui usando o AWS CLI

Use o comando create-resource-share.

Cancelando o compartilhamento de um perfil compartilhado do Route 53

Quando você cancela o compartilhamento de um perfil, as VPCs que têm as configurações desse perfil associadas a elas as perdem e usam como padrão as configurações específicas da VPC.

Para cancelar o compartilhamento de um perfil compartilhado do Route 53 que você possui, você deve removê-lo do compartilhamento de recursos. Você pode fazer isso usando o console do Route 53, o AWS RAM console ou AWS CLI o.

Para cancelar o compartilhamento de um perfil compartilhado do Route 53 que você possui usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Selecione o nome vinculado do Perfil que você deseja cancelar o compartilhamento e, na <Profile name>página, escolha Gerenciar compartilhamento.
4. Você é direcionado ao AWS RAM console, onde pode seguir estas etapas: Atualizar um compartilhamento de recursos no Guia do AWS RAM usuário.

Para cancelar o compartilhamento de um perfil compartilhado do Route 53 que você possui usando o console AWS RAM

Consulte Atualização de um compartilhamento de atributos no Guia do usuário do AWS RAM .

Para cancelar o compartilhamento de um perfil compartilhado do Route 53 que você possui usando o AWS CLI

Use o comando disassociate-resource-share.

Identificação de um perfil compartilhado do Route 53

Proprietários e consumidores podem identificar perfis compartilhados do Route 53 usando o console do Route 53 AWS CLI e.

Para identificar um perfil compartilhado do Route 53 usando o console do Route 53

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Perfis.
3. Se um Perfil for compartilhado com você, a tabela Perfis incluirá o texto Compartilhado comigo.

   Quando você compartilha um Perfil, ele é listado como Compartilhado na tabela Perfis.

Para identificar um perfil compartilhado do Route 53 usando o AWS CLI

Use o comando get-profile ou list-profile. Os comandos retornam informações sobre os Perfis do Route 53 que você possui e o status de compartilhamento dos Perfis do Route 53.

Responsabilidades e permissões para perfis compartilhados do Route 53

Permissões para proprietários

O proprietário do perfil pode visualizar, gerenciar e excluir associações de recursos do perfil, incluindo associações de recursos feitas pelas contas do consumidor. O proprietário pode visualizar e excluir as associações de VPC de sua propriedade. Além disso, somente o proprietário do Perfil pode excluir um Perfil de sua propriedade, e isso também remove automaticamente todas as associações de recursos do Perfil.

Permissões para consumidores

A permissão padrão para consumidores de um perfil compartilhado é somente para leitura. Com permissão somente para leitura, eles podem ver os recursos associados e associá-los às VPCs, mas não podem gerenciar as associações de recursos.

Um proprietário também pode criar permissões gerenciadas pelo cliente no AWS RAM console. Para obter mais informações, consulte Criação e uso de permissões gerenciadas pelo cliente no Guia AWS RAM do usuário.

Faturamento e medição

Os perfis do Route 53 são cobrados com base no número de associações de VPC. O proprietário do perfil é responsável pela cobrança do cliente pelas associações de VPC.

Cotas de instâncias

Os proprietários e consumidores do perfil compartilham a mesma cota, exceto pelo número de perfis do Route 53 por conta em uma região. Para obter mais informações, consulte Cotas nos perfis do Route 53 .

O que é o Amazon Route 53 no Outposts?

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS às instalações do cliente. Isso permite que os clientes executem os serviços da AWS com workloads on-premises usando as mesmas interfaces de programação usadas nas Regiões da AWS. Para obter mais informações, consulte O que é o AWS Outposts? no Guia do usuário do AWS Outposts.

O Route 53 no Outposts oferece dois recursos:

- Um Resolver que armazena em cache todas as consultas ao DNS oriundas do AWS Outposts.
- Conectividade híbrida entre um Outpost e um resolver de DNS on-premises quando você implanta endpoints de entrada e de saída.

Para obter mais informações, consulte O que Amazon Route 53 Resolveré.

Além disso, o Route 53 no Outposts reduz a latência da rede permitindo que as consultas sejam resolvidas no Outpost em vez de precisarem ir e voltar da Região da AWS mais próxima.

> **Note**
>
> Se você tiver uma versão dos racks do AWS Outposts que não for compatível com o Route 53 no Outposts, uma equipe de conta da AWS será notificada e entrará em contato para ajudar você a atualizar o AWS Outposts.

Atributos do Amazon Route 53 no Outposts

A tabela a seguir compara os recursos do Route 53 on Outposts com os recursos do Amazon Route 53.

Comparação do Route 53 no Outposts com o Route 53

Recurso	Disponibilidade no Route 53 no Outposts
Route 53 Resolver	Sim. O Resolver mantém um cache local de registros para aplicações hospedadas no rack do Outpost, na VPC

Recurso	Disponibilidade no Route 53 no Outposts
	emparelhada na Região da AWS e em todos os nomes de host acessíveis ao público.
Verificações de integridade	Não. As verificações de integridade são calculadas e informadas da Região da AWS. Se um Outpost se desconectar da nuvem, ocorrerá uma falha na abertura dos endpoints e não será possível fazer o failover para um backup.
Endpoints do Resolver	Sim. Os endpoints do Resolver no rack do Outpost permitem que as consultas ao DNS sejam encaminhadas e recebidas de servidores DNS on-premises. Apenas o tipo de endpoint IPv4 está disponível para endpoints.
Firewall de DNS do Route 53 Resolver	Não disponível.
Fluxo de tráfego	Não disponível.

Comportamento do Route 53 Resolver quando o AWS Outposts está desconectado da VPC

Se o AWS Outposts estiver desconectado da Região da AWS, o comportamento do Resolver no Outpost é o seguinte:

- Alterações no ambiente de gerenciamento não estão disponíveis.
- As verificações de integridade e o recurso de failover de DNS não estão disponíveis.
- As consultas ao DNS para recursos hospedados localmente nos Outposts são resolvidas, mas, em alguns casos, a resposta pode estar obsoleta se o endereço IP do recurso foi atualizado enquanto o Outpost estava desconectado.
- As consultas ao DNS para recursos hospedados na VPC da região podem ser resolvidas. Porém, os recursos não estarão acessíveis até a conexão do Outpost com a Região da AWS ser restaurada.

- As consultas ao DNS para recursos públicos de DNS podem ser resolvidas se estiverem disponíveis no cache do Route 53 Resolver no Outpost.

Conceitos básicos do Route 53 Resolver no AWS Outposts

Depois que os racks do AWS Outposts forem encomendados e entregues, conforme descrito em Create an AWS Outposts in the AWS Outposts, você poderá configurar o Resolver no Outpost.

Você também pode usar APIs para gerenciar o Route 53 no Outposts. Para obter mais informações, consulte Resolver on Outpost actions.

> **Important**
>
> Pode levar de 30 a 150 minutos para criar um cache do Resolver em um AWS Outposts.

Depois que os racks do AWS Outposts são entregues, você pode optar por usar o Route 53 no Outposts.

Para configurar o Resolver no Outpost

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Na página Resolver no Outpost, escolha Criar Resolver.
5. Na página Criar Resolver:

   - Em AWS Outposts, selecione um AWS Outposts no qual você deseja criar o Resolver.
   - Digite um nome para o Resolver na caixa de texto Nome do Resolver.
   - Depois que Tipos de instância recomendados para o Resolver forem preenchidos com as instâncias do Amazon EC2, escolha uma das opções.

     Para obter mais informações sobre os tipos de instâncias compatíveis, consulte Cotas do Resolver no Outpost.
   - Em Número de instâncias, escolha o número de instâncias de interface elástica para o VPC Resolver. O valor padrão é 4.

Se o seu AWS Outposts não tiver um tipo de instância compatível com o Resolver, você não poderá criar um Resolver.

6. Escolha Criar resolvedor.

   Você pode monitorar a criação do Resolver na página Resolver no Outpost.

Criar endpoints de entrada

Depois de criar um Resolver no Outpost, você pode adicionar endpoints de entrada e de saída para resolver consultas ao DNS enviadas e recebidas pela rede on-premises.

Para configurar endpoints de entrada para o Resolver no Outpost

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Na tabela Endpoints de entrada, escolha Criar endpoint de entrada.
6. Na página Criar endpoint de entrada, insira os valores aplicáveis. Para obter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada em um Outpost.
7. Escolha Criar endpoint.

Valores especificados ao criar ou editar endpoints de entrada em um Outpost

Ao criar ou editar um endpoint de entrada, especifique os seguintes valores:

ID do Outpost

Se você estiver criando o endpoint para um Resolver em uma VPC do AWS Outposts, esse será o ID do AWS Outposts.

Nome do endpoint

Um nome amigável que permite encontrar facilmente um endpoint de entrada no painel.

VPC na Região region-name

Todas as consultas de DNS de entrada da rede passam por essa VPC em direção do Resolver.

Grupo de segurança para este endpoint

O ID de um ou mais grupos de segurança que deseja usar para controlar o acesso a essa VPC. O grupo de segurança especificado deve incluir uma ou mais regras de entrada. As regras de entrada devem permitir o acesso TCP e UDP na porta 53. Não é possível alterar esse valor depois de criar o endpoint.

Para mais informações, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Endereços IP

Os endereços IP para os quais deseja que os resolvedores de DNS encaminhem as consultas de DNS. Exigimos que você especifique um mínimo de dois endereços IP para redundância. Observe o seguinte:

Várias zonas de disponibilidade

É recomendável especificar endereços IP em pelo menos duas zonas de disponibilidade. Opcionalmente, você pode especificar endereços IP adicionais nessas ou em outras zonas de disponibilidade.

Endereços IP e interfaces de rede elástica da Amazon VPC

Para cada combinação de zona de disponibilidade, sub-rede e endereço IP que você especificar, o Resolver criará uma interface de rede elástica da Amazon VPC. Para saber o atual número máximo de consultas de DNS por segundo por endereço IP em um endpoint, consulte Cotas no Route 53 Resolver. Para obter informações sobre os preços de cada interface de rede elástica, consulte “Amazon Route 53”, na página de preços do Amazon Route 53.

> **Note**
>
> O endpoint do Resolver tem um endereço IP privado. Esses endereços IP não mudarão ao longo da vida útil de um endpoint.

Para cada endereço IP, especifique os valores a seguir. Cada endereço IP deve estar em uma zona de disponibilidade na VPC especificada em VPC na região region-name (nome da região).

Zona de disponibilidade

A zona de disponibilidade pelas quais você deseja que as consultas de DNS passem a caminho de sua VPC. A zona de disponibilidade especificada deve ser configurada com uma sub-rede.

Sub-rede

A sub-rede que contém o endereço IP para o qual você deseja encaminhar as consultas de DNS. A sub-rede deve ter um endereço IP disponível.

Especifique a sub-rede para um endereço IPv4. O IPv6 não é compatível.

endereço IP

Um endereço IP para o qual você deseja encaminhar consultas de DNS.

Decida se você quer que o Resolver escolha um endereço IP para você entre os endereços IP disponíveis na sub-rede especificada ou se quer especificar você mesmo o endereço IP.

Se decidir especificar você mesmo o endereço IP, insira um endereço IPv4. O IPv6 não é compatível.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Estas são as tags que o AWS Billing and Cost Management fornece para organizar sua fatura da AWS. Você também pode usar tags para outros fins. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing.

Criar endpoints de saída

Depois de optar por usar e configurar um Route 53 Resolver, você pode adicionar endpoints de entrada e de saída para resolver consultas ao DNS enviadas e recebidas pela rede on-premises.

Para configurar endpoints de saída para o Resolver no Outpost

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Na tabela Endpoints de saída, escolha Criar endpoint de entrada.
6. Na página Criar endpoint de saída, insira os valores aplicáveis. Para obter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada em um Outpost.
7. Escolha Criar endpoint.

Os valores especificados ao criar ou editar endpoints de saída em um AWS Outposts

Ao criar ou editar um endpoint de entrada, especifique os seguintes valores:

ID do Outpost

Se você estiver criando o endpoint para um Resolver em uma VPC do AWS Outposts, esse será o ID do AWS Outposts.

Nome do endpoint

Um nome amigável que permite encontrar facilmente um endpoint de entrada no painel.

VPC na Região region-name

Todas as consultas de DNS de entrada da rede passam por essa VPC em direção do Resolver.

Grupo de segurança para este endpoint

O ID de um ou mais grupos de segurança que deseja usar para controlar o acesso a essa VPC. O grupo de segurança especificado deve incluir uma ou mais regras de entrada. As regras de entrada devem permitir o acesso TCP e UDP na porta 53. Não é possível alterar esse valor depois de criar o endpoint.

Para mais informações, consulte Grupos de segurança para a VPC no Guia do usuário da Amazon VPC.

Endereços IP

Os endereços IP para os quais deseja que os resolvedores de DNS encaminhem as consultas de DNS. Exigimos que você especifique um mínimo de dois endereços IP para redundância. Observe o seguinte:

Várias zonas de disponibilidade

É recomendável especificar endereços IP em pelo menos duas zonas de disponibilidade. Opcionalmente, você pode especificar endereços IP adicionais nessas ou em outras zonas de disponibilidade.

Endereços IP e interfaces de rede elástica da Amazon VPC

Para cada combinação de zona de disponibilidade, sub-rede e endereço IP que você especificar, o Resolver criará uma interface de rede elástica da Amazon VPC. Para saber o atual número máximo de consultas de DNS por segundo por endereço IP em um endpoint, consulte Cotas no Route 53 Resolver. Para obter informações sobre os preços de cada interface de rede elástica, consulte “Amazon Route 53”, na página de preços do Amazon Route 53.

> **Note**
>
> O endpoint do Resolver tem um endereço IP privado. Esses endereços IP não mudarão ao longo da vida útil de um endpoint.

Para cada endereço IP, especifique os valores a seguir. Cada endereço IP deve estar em uma zona de disponibilidade na VPC especificada em VPC na região region-name (nome da região).

Zona de disponibilidade

A zona de disponibilidade pelas quais você deseja que as consultas de DNS passem a caminho de sua VPC. A zona de disponibilidade especificada deve ser configurada com uma sub-rede.

Sub-rede

A sub-rede que contém o endereço IP para o qual você deseja encaminhar as consultas de DNS. A sub-rede deve ter um endereço IP disponível.

Especifique a sub-rede para um endereço IPv4. O IPv6 não é compatível.

endereço IP

Um endereço IP para o qual você deseja encaminhar consultas de DNS.

Decida se você quer que o Resolver escolha um endereço IP para você entre os endereços IP disponíveis na sub-rede especificada ou se quer especificar você mesmo o endereço IP.

Se decidir especificar você mesmo o endereço IP, insira um endereço IPv4. O IPv6 não é compatível.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Estas são as tags que o AWS Billing and Cost Management fornece para organizar sua fatura da AWS. Você também pode usar tags para outros fins. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing.

Criar regras de encaminhamento para endpoints de saída

Você também pode criar regras de encaminhamento para endpoints de saída. Para obter mais informações, consulte Para criar regras de encaminhamento e associá-las a uma ou mais VPCs.

Gerenciar um Resolver no Outpost

Para gerenciar um Resolver no Outpost, siga o procedimento aplicável.

Tópicos

- Editar um Resolver no Outpost
- Visualizar o status do Resolver no Outpost
- Excluir um Resolver no Outpost

Editar um Resolver no Outpost

Para editar um Resolver no Outpost, faça o procedimento a seguir.

Para editar um Resolver no Outpost

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Editar.
5. Você pode editar as seguintes informações:
   - O nome do Resolver
   - O tipo de instância
   - O número de instâncias do
6. Depois que terminar de editar, escolha Salvar alterações.

Visualizar o status do Resolver no Outpost

Para visualizar o status de um Resolver no Outpost, faça o procedimento a seguir.

Como exibir o status de um endpoint de entrada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. A coluna Status na página Resolver no Outpost contém um dos seguintes valores:

   Creating (Criando)

   O Resolver no Outpost está em processo de criação.

   Operacional

   O Resolver no Outpost está configurado corretamente.

Atualizando

O Resolver no Outpost está atualizando os tipos de instância.

Ação necessária

Esse endpoint não está íntegro e não pode ser recuperado automaticamente. Para resolver o problema, recomendamos que você verifique se o AWS Outposts da instância é compatível com o Resolver no Outpost.

Deleting (Excluindo)

O Resolver no Outpost está em processo de exclusão.

Falha na criação

A criação do Resolver no Outpost falhou.

Falha na exclusão

A exclusão do Resolver no Outpost falhou. Para corrigir esse problema, tente novamente em alguns minutos.

Excluir um Resolver no Outpost

> **Note**
>
> Antes de excluir um Resolver no Outpost, você deve primeiro excluir todos os endpoints associados a ele.

Para excluir um Resolver no Outpost, faça o procedimento a seguir.

Para excluir um Resolver no Outpost

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Excluir.

5. Na caixa de diálogo Excluir Resolver, insira **`delete`** na caixa de texto e selecione Excluir.

Gerenciar endpoints de entrada no Resolver no Outpost

Para gerenciar endpoints de entrada no Resolver no Outpost, siga o procedimento aplicável.

Tópicos

Visualizar e editar endpoints de entrada

Para visualizar e editar as configurações de um endpoint de entrada, execute o procedimento a seguir.

Para visualizar e editar as configurações de um endpoint de entrada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Na lista Endpoints de entrada, escolha a opção de endpoint cujas configurações você deseja visualizar ou editar.
6. Escolha View details (Visualizar detalhes) ou Edit (Editar).

   Para obter informações sobre os valores dos endpoints de entrada, consulte Valores especificados ao criar ou editar endpoints de entrada em um Outpost.
7. Se você escolheu Edit (Editar), insira os valores aplicáveis e selecione Save (Salvar).

Visualizar o status dos endpoints de entrada

Para visualizar o status de um endpoint de entrada, realize o procedimento a seguir.

Como exibir o status de um endpoint de entrada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. A coluna Status da lista de endpoints de entrada contém um dos seguintes valores:

   Creating (Criando)

   O Resolver está criando e configurando uma ou mais interfaces de rede da Amazon VPC para esse endpoint.

   Operacional

   As interfaces de rede da Amazon VPC para esse endpoint estão configuradas corretamente e são capazes de passar consultas de DNS de entrada ou de saída entre a rede e o Resolver.

   Atualizando

   O resolvedor está associando ou desassociando uma ou mais interfaces de rede com esse endpoint.

   Recuperação automática

   O Resolver está tentando recuperar uma ou mais interfaces de rede associadas a esse endpoint. Durante o processo de recuperação, o endpoint funciona com capacidade limitada por causa do limite do número de consultas de DNS por endereço IP (por interface de rede). Para obter o limite atual, consulte Cotas no Route 53 Resolver.

   Ação necessária

   Esse endpoint não é íntegro, e o Resolver não pode recuperá-lo automaticamente. Para resolver o problema, recomendamos que você verifique cada endereço IP associado ao endpoint. Para cada endereço IP que não está disponível, adicione outro endereço IP e exclua o endereço IP que não está disponível. Um endpoint sempre deve incluir pelo menos dois endereços IP. Um status de Action needed (Ação necessária) pode ter várias causas. Aqui estão duas causas comuns:

- Uma ou mais interfaces de rede associadas ao endpoint foram excluídas usando a Amazon VPC.
- A interface de rede não pôde ser criada por algum motivo que está fora do controle do Resolver.

Deleting (Excluindo)

O resolvedor está excluindo esse endpoint e as interfaces de rede associadas.

Excluir endpoints de entrada

Para excluir um endpoint de entrada, execute o seguinte procedimento.

> **Important**
>
> Se você excluir um endpoint de entrada, as consultas de DNS da sua rede não serão mais encaminhadas para o Resolver na VPC especificada no endpoint.

Para excluir um endpoint de entrada

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Marque a caixa de seleção ao lado do endpoint que você deseja excluir.
6. Escolha Delete (Excluir).
7. Para confirmar a exclusão do endpoint, insira o nome do endpoint e escolha Submit (Enviar).

Gerenciar endpoints de saída no Resolver no Outpost

Para gerenciar endpoints de saída no Resolver no Outpost, siga o procedimento aplicável.

Tópicos

Visualizar e editar endpoints de saída

Para visualizar e editar as configurações de um endpoint de saída, execute o procedimento a seguir.

Para visualizar e editar as configurações de um endpoint de saída

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.
4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Na lista Endpoints de saída, marque a caixa de seleção ao lado do endpoint cujas configurações você deseja visualizar ou editar.
6. Escolha View details (Visualizar detalhes) ou Edit (Editar).

   Para obter informações sobre os valores dos endpoints de saída, consulte Os valores especificados ao criar ou editar endpoints de saída em um AWS Outposts.
7. Se você escolheu Edit (Editar), insira os valores aplicáveis e, em seguida, selecione Save (Salvar).

Visualizar o status dos endpoints de saída

Para visualizar o status de um endpoint de saída, realize o procedimento a seguir.

Como visualizar o status de um endpoint de saída

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Na barra de navegação, escolha a região em que o AWS Outposts está localizado.

4. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
5. Na lista de endpoints de entrada, a coluna Status contém um dos seguintes valores:

   Creating (Criando)

   O Resolver está criando e configurando uma ou mais interfaces de rede da Amazon VPC para esse endpoint.

   Operacional

   As interfaces de rede da Amazon VPC para esse endpoint estão configuradas corretamente e são capazes de passar consultas de DNS de entrada ou de saída entre a rede e o Resolver.

   Atualizando

   O resolvedor está associando ou desassociando uma ou mais interfaces de rede com esse endpoint.

   Recuperação automática

   O Resolver está tentando recuperar uma ou mais interfaces de rede associadas a esse endpoint. Durante o processo de recuperação, o endpoint funciona com capacidade limitada por causa do limite do número de consultas de DNS por endereço IP (por interface de rede). Para obter o limite atual, consulte Cotas no Route 53 Resolver.

   Ação necessária

   Esse endpoint não é íntegro, e o Resolver não pode recuperá-lo automaticamente. Para resolver o problema, recomendamos que você verifique cada endereço IP associado ao endpoint. Para cada endereço IP que não está disponível, adicione outro endereço IP e exclua o endereço IP que não está disponível. (Um endpoint sempre deve incluir pelo menos dois endereços IP.) Um status de Action needed (Ação necessária) pode ter várias causas. Aqui estão duas causas comuns:

   - Uma ou mais interfaces de rede associadas ao endpoint foram excluídas usando a Amazon VPC.
   - A interface de rede não pôde ser criada por algum motivo que está fora do controle do Resolver.

Deleting (Excluindo)

O resolvedor está excluindo esse endpoint e as interfaces de rede associadas.

Excluir endpoints de saída

Antes de excluir um endpoint, você deve primeiro excluir todas as regras associadas a uma VPC.

Para excluir um endpoint de saída, execute o seguinte procedimento.

> **Important**
>
> Se você excluir um endpoint de saída, o Resolver irá parar de encaminhar consultas de DNS de sua VPC à rede para regras que especificam o endpoint de saída excluído.

Para excluir um endpoint de saída

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação esquerdo, expanda Resolver e navegue até Outposts.
3. Marque a caixa de seleção ao lado do Resolver que está no estado operacional e escolha Visualizar detalhes.
4. Na lista Endpoints de saída, escolha a opção para o endpoint que você deseja excluir.
5. Escolha Delete (Excluir).
6. Para confirmar a exclusão do endpoint, insira o nome do endpoint e, em seguida, escolha Submit (Enviar).

Como criar recursos do Amazon Route 53 e do Amazon Route 53 Resolver com o AWS CloudFormation

O Amazon Route 53 e o Amazon Route 53 Resolver são integrados ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS para que você possa passar menos tempo criando e gerenciando os recursos e a infraestrutura. Você cria um modelo que descreve todos os recursos da AWS desejados, e o AWS CloudFormation provisiona e configura esses recursos para você.

Quando você usa o AWS CloudFormation, é possível reutilizar seu modelo para configurar seus recursos do Route 53 e do Route 53 Resolver repetidamente, e de forma consistente. Descreva seus recursos uma vez e, depois, provisione os mesmos recursos repetidamente em várias regiões e nas Contas da AWS.

Route 53, Route 53 Resolver e modelos do AWS CloudFormation

Para provisionar e configurar recursos para o Route 53, o Route 53 Resolver e serviços relacionados, você deve entender os modelos do AWS CloudFormation. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do AWS CloudFormation. Para obter mais informações, consulte O que é o Designer? (O que é o AWS CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

O Route 53 oferece suporte para criar os seguintes tipos de recursos no AWS CloudFormation:

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para recursos do Route 53, consulte a Referência de tipo de recurso do Amazon Route 53 no Manual do usuário do AWS CloudFormation.

O Route 53 Resolver oferece suporte para criação dos seguintes tipos de recursos no 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`

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para recursos do Route 53 Resolver, consulte a Referência de tipo de recurso do Amazon Route 53 Resolver no Manual do usuário do AWS CloudFormation.

Saiba mais sobre o AWS CloudFormation

Para saber mais sobre o AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- AWS CloudFormation Referência da API
- Guia do usuário da interface de linha de comando do AWS CloudFormation

Exemplos de código para o Route 53 usando SDKs da AWS

Os exemplos de código a seguir mostram como usar o Route 53 com um kit de desenvolvimento de software (SDK) da AWS.

Para obter uma lista completa dos guias do desenvolvedor do SDK da AWS e exemplos de código, consulte Usando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código

- Comece a usar o registro de domínio do Route 53 usando um AWS SDK

Exemplos de código para o Route 53 usando AWS SDKs

Os exemplos de código a seguir mostram como usar o Route 53 com um kit AWS de desenvolvimento de software (SDK).

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar funções de serviço específicas, é possível ver as ações contextualizadas em seus devidos cenários e exemplos entre serviços.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código

- Ações para o Route 53 usando AWS SDKs
  - Use ChangeResourceRecordSets com um AWS SDK ou CLI
  - Use CreateHostedZone com um AWS SDK ou CLI
  - Use DeleteHostedZone com um AWS SDK ou CLI
  - Use GetHostedZone com um AWS SDK ou CLI
  - Use ListHostedZones com um AWS SDK ou CLI
  - Use ListHostedZonesByName com um AWS SDK ou CLI
  - Use ListQueryLoggingConfigs com um AWS SDK ou CLI

Ações para o Route 53 usando AWS SDKs

Os exemplos de código a seguir demonstram como realizar ações individuais do Route 53 com AWS SDKs. Esses trechos chamam a API do Route 53 e são trechos de código de programas maiores que devem ser executados no contexto. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para uma lista completa, consulte a Amazon Route 53 API Reference.

Exemplos

- Use ChangeResourceRecordSets com um AWS SDK ou CLI
- Use CreateHostedZone com um AWS SDK ou CLI
- Use DeleteHostedZone com um AWS SDK ou CLI
- Use GetHostedZone com um AWS SDK ou CLI
- Use ListHostedZones com um AWS SDK ou CLI
- Use ListHostedZonesByName com um AWS SDK ou CLI
- Use ListQueryLoggingConfigs com um AWS SDK ou CLI

Use **`ChangeResourceRecordSets`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ChangeResourceRecordSets`.

CLI

AWS CLI

Para criar, atualizar ou excluir um conjunto de registros de recursos

O `change-resource-record-sets` comando a seguir cria um conjunto de registros de recursos usando a `hosted-zone-id` `Z1R8UBAEXAMPLE` e a configuração formatada em JSON no arquivo: `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
```

Para obter mais informações, consulte POST ChangeResourceRecordSets na Amazon Route 53 API Reference.

A configuração no arquivo JSON depende do tipo de conjunto de registros de recursos que você deseja criar:

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Pseudônimo

Sintaxe básica:

```
{
  "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"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

Sintaxe ponderada:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintaxe do 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"
      }
    },
    {...}
  ]
}
```

Sintaxe ponderada do alias:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "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"
      }
    },
    {...}
  ]
}
```

Sintaxe de latência:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintaxe do alias de latência:

```
{
  "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"
      }
    },
    {...}
  ]
}
```

Sintaxe de 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"
      }
    },
    {...}
```

```
  ]
}
```

Sintaxe do alias de 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"
      }
    },
    {...}
  ]
}
```

- Para obter detalhes da API, consulte ChangeResourceRecordSetsna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo cria um registro A para www.example.com e altera o registro A para test.example.com de 192.0.2.3 para 192.0.2.1. Observe que os valores dos registros do tipo TXT de alterações devem estar entre aspas duplas. Consulte a documentação do Amazon

Route 53 para obter mais detalhes. Você pode usar o Get-R53Change cmdlet para pesquisar para determinar quando as alterações foram concluídas.

```
$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
```

Exemplo 2: Este exemplo mostra como criar conjuntos de registros de recursos de alias. 'Z222222222' é o ID da zona hospedada do Amazon Route 53 na qual você está criando o conjunto de registros do recurso alias. 'exemplo.com' é o ápice da zona para o qual você deseja criar um alias e 'www.exemplo.com' é um subdomínio para o qual você também deseja criar um alias. 'Z1111111111111' é um exemplo de ID de zona hospedada para o balanceador de carga e 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com' é um exemplo

de nome de domínio do balanceador de carga com o qual o Amazon Route 53 responde às consultas de example.com e www.example.com. Consulte a documentação do Amazon Route 53 para obter mais detalhes. Você pode usar o Get-R53Change cmdlet para pesquisar para determinar quando as alterações foram concluídas.

```
$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
```

Exemplo 3: Este exemplo cria dois registros A para www.example.com. Um quarto das vezes (1/ (1+3)), o Amazon Route 53 responde às consultas de www.example.com com os dois valores do primeiro conjunto de registros de recursos (192.0.2.9 e 192.0.2.10). Três quartos

das vezes (3/ (1+3)) O Amazon Route 53 responde às consultas de www.example.com com os dois valores para o segundo conjunto de registros de recursos (192.0.2.11 e 192.0.2.12). Consulte a documentação do Amazon Route 53 para obter mais detalhes. Você pode usar o Get-R53Change cmdlet para pesquisar para determinar quando as alterações foram concluídas.

```
$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
```

Exemplo 4: Este exemplo mostra como criar conjuntos de registros de recursos de alias ponderados, supondo que example.com seja o domínio para o qual você deseja criar conjuntos de registros de recursos de alias ponderados. SetIdentifier diferencia os dois conjuntos de registros de recursos de alias ponderados um do outro. Esse elemento é necessário porque os elementos Nome e Tipo têm os mesmos valores para os dois conjuntos

de registros de recursos. Z11111111111 e Z333333333333333 são exemplos de IDs de zona hospedada para o balanceador de carga ELB especificado pelo valor de DNSName. example-load-balancer-22222222.us-east-1.elb.amazonaws.com e example-load-balancer-4444444444.us-east-1.elb.amazonaws.com são exemplos de domínios do Elastic Load Balancing dos quais o Amazon Route 53 responde a consultas de example.com. Consulte a documentação do Amazon Route 53 para obter mais detalhes. Você pode usar o Get-R53Change cmdlet para pesquisar para determinar quando as alterações foram concluídas.

```
$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
```

Exemplo 5: Este exemplo cria dois conjuntos de registros de recursos de alias de latência, um para um balanceador de carga ELB na região Oeste dos EUA (Oregon) (us-west-2) e outro para um balanceador de carga na região Ásia-Pacífico (Cingapura) (ap-southeast-1). Consulte a documentação do Amazon Route 53 para obter mais detalhes. Você pode usar o Get-R53Change cmdlet para pesquisar para determinar quando as alterações foram concluídas.

```
$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
```

- Para obter detalhes da API, consulte ChangeResourceRecordSetsem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`CreateHostedZone`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `CreateHostedZone`.

CLI

AWS CLI

Para criar uma hosted zone

O `create-hosted-zone` comando a seguir adiciona uma zona hospedada chamada `example.com` usando a referência `2014-04-01-18:47` do chamador. O comentário opcional inclui um espaço, portanto, ele deve estar entre aspas:

```
aws route53 create-hosted-zone --name example.com --caller-reference
 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

Para obter mais informações, consulte Como trabalhar com zonas hospedadas no Guia do desenvolvedor do Amazon Route 53.

- Para obter detalhes da API, consulte CreateHostedZonena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: cria uma nova zona hospedada chamada 'example.com', associada a um conjunto de delegações reutilizável. Observe que você deve fornecer um valor para o CallerReference

parâmetro para que as solicitações precisem ser repetidas, se necessário, sem o risco de executar a operação duas vezes. Como a zona hospedada está sendo criada em uma VPC, ela é automaticamente privada e você não deve definir o parâmetro - 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
```

- Para obter detalhes da API, consulte CreateHostedZoneem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DeleteHostedZone`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DeleteHostedZone`.

CLI

AWS CLI

Para excluir uma zona hospedada

O `delete-hosted-zone` comando a seguir exclui a zona hospedada com um `id` de`Z36KTIQEXAMPLE`:

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- Para obter detalhes da API, consulte DeleteHostedZonena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Exclui a zona hospedada com o ID especificado. Você será solicitado a confirmar antes que o comando continue, a menos que você adicione o parâmetro -Force switch.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- Para obter detalhes da API, consulte DeleteHostedZoneem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetHostedZone`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetHostedZone`.

CLI

AWS CLI

Para obter informações sobre uma zona hospedada

O `get-hosted-zone` comando a seguir obtém informações sobre a zona hospedada com um `id` dos`Z1R8UBAEXAMPLE`:

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- Para obter detalhes da API, consulte GetHostedZonena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Retorna detalhes da zona hospedada com a ID Z1D633PJN98FT9.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- Para obter detalhes da API, consulte GetHostedZoneem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListHostedZones`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListHostedZones`.

CLI

AWS CLI

Para listar as zonas hospedadas associadas à AWS conta atual

O `list-hosted-zones` comando a seguir lista informações resumidas sobre as primeiras 100 zonas hospedadas associadas à AWS conta atual. :

```
aws route53 list-hosted-zones
```

Se você tiver mais de 100 zonas hospedadas ou se quiser listá-las em grupos de menos de 100 zonas, inclua o parâmetro `--max-items`. Por exemplo, para listar as zonas hospedadas, use o seguinte comando:

```
aws route53 list-hosted-zones --max-items 1
```

Para visualizar informações sobre a próxima zona hospedada, pegue o valor de `NextToken` da resposta ao comando anterior e inclua-o no parâmetro `--starting-token`, por exemplo:

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- Para obter detalhes da API, consulte ListHostedZonesna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: gera todas as suas zonas hospedadas públicas e privadas.

```
Get-R53HostedZoneList
```

Exemplo 2: Exibe todas as zonas hospedadas associadas ao conjunto de delegações reutilizáveis que tem a ID NZ8X2CISAMPLE

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- Para obter detalhes da API, consulte ListHostedZonesem Referência de AWS Tools for PowerShell cmdlet.

Rust

SDK para Rust

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
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(())
}
```

- Para obter detalhes da API, consulte a ListHostedZonesreferência da API AWS SDK for Rust.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListHostedZonesByName`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListHostedZonesByName`.

CLI

AWS CLI

O comando a seguir lista até 100 zonas hospedadas ordenadas por nome de domínio:

```
aws route53 list-hosted-zones-by-name
```

Saída:

```
{
  "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"
}
```

O comando a seguir lista as zonas hospedadas ordenadas por nome, começando com`www.example.com`:

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

Saída:

```
{
    "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"
}
```

- Para obter detalhes da API, consulte ListHostedZonesByNamena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: retorna todas as suas zonas hospedadas públicas e privadas em ordem ASCII por nome de domínio.

```
Get-R53HostedZonesByName
```

Exemplo 2: retorna suas zonas hospedadas públicas e privadas, em ordem ASCII por nome de domínio, começando pelo nome DNS especificado.

```
Get-R53HostedZonesByName -DnsName example2.com
```

Exemplo 3: Este exemplo mostra como enumerar manualmente as zonas hospedadas recuperando primeiro um único item e depois iterando dois por vez até que todas as zonas tenham sido retornadas, usando propriedades de marcador anexadas à resposta do serviço na pilha após cada chamada. **$AWSHistory**

```
Get-R53HostedZonesByName -MaxItem 1
while ($LastServiceResponse.IsTruncated)
{
    $nextPageParams = @{
        DnsName=$LastServiceResponse.NextDNSName
        HostedZoneId=$LastServiceResponse.NextHostedZoneId
    }
    Get-R53HostedZonesByName -MaxItem 2 @nextPageParams
}
```

- Para obter detalhes da API, consulte ListHostedZonesByNameem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListQueryLoggingConfigs`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListQueryLoggingConfigs`.

CLI

AWS CLI

Para listar as configurações de registro de consultas

O `list-query-logging-configs` exemplo a seguir lista informações sobre as primeiras 100 configurações de registro de consultas em sua AWS conta, para a zona `Z1OX3WQEXAMPLE` hospedada.

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

Saída:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

Para obter mais informações, consulte Registro de consultas de DNS no Amazon Route 53 Developer Guide.

- Para obter detalhes da API, consulte ListQueryLoggingConfigsna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo retorna todas as configurações do registro de consultas DNS associadas à atual. Conta da AWS

```
Get-R53QueryLoggingConfigList
```

Saída:

```
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:*
```

- Para obter detalhes da API, consulte ListQueryLoggingConfigsem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código para registro de domínio do Route 53 usando AWS SDKs

Os exemplos de código a seguir mostram como usar o registro de domínio do Route 53 com um kit AWS de desenvolvimento de software (SDK).

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar funções de serviço específicas, é possível ver as ações contextualizadas em seus devidos cenários e exemplos entre serviços.

Cenários são exemplos de código que mostram como realizar uma tarefa específica chamando várias funções dentro do mesmo serviço.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Conceitos básicos

Registro de domínios do Olá, Route 53

O exemplo de código a seguir mostra como começar a usar o registro de domínios do Route 53.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}");
        }
    }
}
```

- Para obter detalhes da API, consulte ListPricesa Referência AWS SDK for .NET da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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);
        }
    }
}
```

- Para obter detalhes da API, consulte ListPricesa Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
/**
 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}")
            }
    }
```

```
}
```

- Para obter detalhes da API, consulte a ListPricesreferência da API AWS SDK for Kotlin.

Exemplos de código

- Ações para registro de domínio do Route 53 usando AWS SDKs
  - Use CheckDomainAvailability com um AWS SDK ou CLI
  - Use CheckDomainTransferability com um AWS SDK ou CLI
  - Use GetDomainDetail com um AWS SDK ou CLI
  - Use GetDomainSuggestions com um AWS SDK ou CLI
  - Use GetOperationDetail com um AWS SDK ou CLI
  - Use ListDomains com um AWS SDK ou CLI
  - Use ListOperations com um AWS SDK ou CLI
  - Use ListPrices com um AWS SDK ou CLI
  - Use RegisterDomain com um AWS SDK ou CLI
  - Use ViewBilling com um AWS SDK ou CLI
- Cenários para registro de domínio do Route 53 usando AWS SDKs
  - Comece a usar o registro de domínio do Route 53 usando um AWS SDK

Ações para registro de domínio do Route 53 usando AWS SDKs

Os exemplos de código a seguir demonstram como realizar ações individuais de registro de domínio do Route 53 com AWS SDKs. Esses trechos chamam a API do registro de domínios do Route 53 e são trechos de código de programas maiores que devem ser executados no contexto. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a Referência de APIs do Amazon Route 53 domain registration.

Exemplos

- Use CheckDomainAvailability com um AWS SDK ou CLI
- Use CheckDomainTransferability com um AWS SDK ou CLI
- Use GetDomainDetail com um AWS SDK ou CLI

- Use GetDomainSuggestions com um AWS SDK ou CLI
- Use GetOperationDetail com um AWS SDK ou CLI
- Use ListDomains com um AWS SDK ou CLI
- Use ListOperations com um AWS SDK ou CLI
- Use ListPrices com um AWS SDK ou CLI
- Use RegisterDomain com um AWS SDK ou CLI
- Use ViewBilling com um AWS SDK ou CLI

Use **`CheckDomainAvailability`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `CheckDomainAvailability`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
/// <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;
    }
```

- Para obter detalhes da API, consulte CheckDomainDisponibilidade na Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para determinar se você pode registrar um nome de domínio com o Route 53

O `check-domain-availability` comando a seguir retorna informações sobre se o nome de domínio `example.com` está disponível para ser registrado usando o Route 53.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

Saída:

```
{
    "Availability": "UNAVAILABLE"
}
```

O Route 53 oferece suporte a um grande número de domínios de primeiro nível (TLDs), como `.com` e`.jp`, mas não oferecemos suporte a todos os TLDs disponíveis. Se você verificar a disponibilidade de um domínio e o Route 53 não suportar o TLD, `check-domain-availability` retornará a seguinte mensagem.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Para obter uma lista dos TLDs que você pode usar ao registrar um domínio no Route 53, consulte Domains That You Can Register with Amazon Route 53 no Amazon Route 53 Developer Guide. Para obter mais informações sobre o registro de domínios no Amazon Route 53, consulte Registro de um novo domínio no Guia do desenvolvedor do Amazon Route 53.

- Para obter detalhes da API, consulte CheckDomainDisponibilidade na Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte CheckDomainDisponibilidade na Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
    }
}
```

- Para obter detalhes da API, consulte CheckDomainDisponibilidade no AWS SDK para referência da API Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`CheckDomainTransferability`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `CheckDomainTransferability`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
/// <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;
}
```

- Para obter detalhes da API, consulte CheckDomainTransferibilidade na Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para determinar se um domínio pode ser transferido para o Route 53

O `check-domain-transferability` comando a seguir retorna informações sobre se você pode transferir o nome de domínio `example.com` para o Route 53.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

Saída:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

Para obter mais informações, consulte Transferência do registro de um domínio para o Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

- Para obter detalhes da API, consulte CheckDomainTransferibilidade na Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
        }
    }
```

- Para obter detalhes da API, consulte CheckDomainTransferibilidade na Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
    }
}
```

- Para obter detalhes da API, consulte CheckDomainTransferabilidade no AWS SDK para referência da API Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetDomainDetail`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetDomainDetail`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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.";
        }
    }
```

- Para obter detalhes da API, consulte GetDomainDetalhes na Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para obter informações detalhadas sobre um domínio especificado

O `get-domain-detail` comando a seguir exibe informações detalhadas sobre o domínio especificado.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

Saída:

```
{
    "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"
    ]
}
```

- Para obter detalhes da API, consulte GetDomainDetalhes na Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
        }
    }
```

- Para obter detalhes da API, consulte GetDomainDetalhes na Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
    }
}
```

- Para obter detalhes da API, consulte GetDomainDetalhe no AWS SDK para referência da API Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetDomainSuggestions`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetDomainSuggestions`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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;
    }
```

- Para obter detalhes da API, consulte GetDomainSugestões na Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para obter uma lista de nomes de domínio sugeridos

O `get-domain-suggestions` comando a seguir exibe uma lista de nomes de domínio sugeridos com base no nome do domínio`example.com`. A resposta inclui somente nomes de domínio que estão disponíveis. Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

Saída:


```
{
    "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"
        }
    ]
}
```

- Para obter detalhes da API, consulte GetDomainSugestões na Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte GetDomainSugestões na Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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(" ")
        }
    }
}
```

- Para obter detalhes da API, consulte GetDomainSugestões no AWS SDK para referência da API Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetOperationDetail`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetOperationDetail`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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}.";
        }
    }
```

- Para obter detalhes da API, consulte GetOperationDetalhes na Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para obter o status atual de uma operação

Algumas operações de registro de domínio operam de forma assíncrona e retornam uma resposta antes de serem concluídas. Essas operações retornam um ID de operação que você pode usar para obter o status atual. O `get-operation-detail` comando a seguir retorna o status da operação especificada.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

Saída:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
```

```
}
```

- Para obter detalhes da API, consulte GetOperationDetalhes na Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte GetOperationDetalhes na Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
    }
}
```

- Para obter detalhes da API, consulte GetOperationDetalhe no AWS SDK para referência da API Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListDomains`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListDomains`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
/// <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;
}
```

- Para obter detalhes da API, consulte ListDomainsa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para listar os domínios que estão registrados com a conta atual AWS

O `list-domains` comando a seguir lista informações resumidas sobre os domínios registrados na AWS conta atual.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains list-domains
    --region us-east-1
```

Saída:

```
{
    "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
        }
    ]
}
```

- Para obter detalhes da API, consulte ListDomainsem Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    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);
        }
    }
```

- Para obter detalhes da API, consulte ListDomainsa Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
            }
    }
}
```

- Para obter detalhes da API, consulte a ListDomainsreferência da API AWS SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListOperations`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListOperations`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   /// <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;
    }
```

- Para obter detalhes da API, consulte ListOperationsa Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para listar o status das operações que retornam um ID de operação

Algumas operações de registro de domínio são executadas de forma assíncrona e retornam uma resposta antes de serem concluídas. Essas operações retornam um ID de operação que você pode usar para obter o status atual. O `list-operations` comando a seguir lista informações resumidas, incluindo o status, sobre as operações atuais de registro de domínio.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains list-operations
    --region us-east-1
```

Saída:

```
{
    "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
        }
    ]
}
```

A saída inclui todas as operações que retornam um ID de operação e que você executou em todos os domínios que você já registrou usando a AWS conta atual. Se quiser obter somente as operações enviadas após uma data especificada, você pode incluir o `submitted-since` parâmetro e especificar uma data no formato Unix e no Horário Universal Coordenado (UTC). O comando a seguir obtém o status de todas as operações enviadas após as 12h UTC de 1º de janeiro de 2020.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- Para obter detalhes da API, consulte ListOperationsem Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte ListOperationsa Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
            }
    }
}
```

- Para obter detalhes da API, consulte a ListOperationsreferência da API AWS SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use `ListPrices` com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ListPrices`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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();
    }
```

- Para obter detalhes da API, consulte ListPricesa Referência AWS SDK for .NET da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
       }
   }
```

- Para obter detalhes da API, consulte ListPricesa Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
            }
    }
}
```

- Para obter detalhes da API, consulte a ListPricesreferência da API AWS SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`RegisterDomain`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `RegisterDomain`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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;
        }
    }
```

- Para obter detalhes da API, consulte RegisterDomaina Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para registrar um domínio

O `register-domain` comando a seguir registra um domínio, recuperando todos os valores dos parâmetros de um arquivo formatado em JSON.

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

Conteúdo de `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
}
```

Saída:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

Para confirmar que a operação foi bem-sucedida, você pode executar`get-operation-detail`. Para obter mais informações, consulte get-operation-detail.

Para obter mais informações, consulte Registrar um novo domínio no Guia do desenvolvedor do Amazon Route 53.

Para obter informações sobre quais domínios de primeiro nível (TLDs) exigem valores `ExtraParams` e quais são os valores válidos, consulte ExtraParama Amazon Route 53 API Reference.

- Para obter detalhes da API, consulte RegisterDomainem Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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 "";
    }
```

- Para obter detalhes da API, consulte RegisterDomaina Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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
    }
}
```

- Para obter detalhes da API, consulte a RegisterDomainreferência da API AWS SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ViewBilling`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `ViewBilling`.

Exemplos de ações são trechos de código de programas maiores e devem ser executados em contexto. É possível ver essa ação no contexto no seguinte exemplo de código:

- Conceitos básicos de domínios

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <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;
    }
```

- Para obter detalhes da API, consulte ViewBillinga Referência AWS SDK for .NET da API.

CLI

AWS CLI

Para obter informações de cobrança das cobranças de registro de domínio da conta corrente AWS

O `view-billing` comando a seguir retorna todos os registros de cobrança relacionados ao domínio da conta corrente no período de 1º de janeiro de 2018 (1514764800 no horário Unix) e meia-noite de 31 de dezembro de 2019 (1577836800 no horário Unix).

Esse comando é executado somente na `us-east-1` região. Se sua região padrão estiver definida como`us-east-1`, você poderá omitir o `region` parâmetro.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

Saída:

```
{
    "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
        }
    ]
}
```

Para obter mais informações, consulte ViewBillinga Referência de API do Amazon Route 53.

- Para obter detalhes da API, consulte ViewBillingem Referência de AWS CLI Comandos.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   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);
        }
    }
```

- Para obter detalhes da API, consulte ViewBillinga Referência AWS SDK for Java 2.x da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
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}")
            }
    }
}
```

- Para obter detalhes da API, consulte a ViewBillingreferência da API AWS SDK for Kotlin.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Cenários para registro de domínio do Route 53 usando AWS SDKs

Os exemplos de código a seguir mostram como implementar cenários comuns no registro de domínio do Route 53 com AWS SDKs. Esses cenários mostram como realizar tarefas específicas chamando várias funções no registro de domínios do Route 53. Cada cenário inclui um link para GitHub, onde você pode encontrar instruções sobre como configurar e executar o código.

Exemplos

- Comece a usar o registro de domínio do Route 53 usando um AWS SDK

Comece a usar o registro de domínio do Route 53 usando um AWS SDK

Os exemplos de código a seguir mostram como:

- Liste os domínios atuais e as operações do ano passado.
- Ver o faturamento do ano passado e os preços dos tipos de domínio.
- Receber sugestões de domínio.
- Verificar a disponibilidade e a transferibilidade de um domínio.
- Opcionalmente, solicitar o registro de um domínio.
- Obter os detalhes de uma operação.
- Opcionalmente, obter os detalhes de um domínio.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Execute um cenário interativo em um prompt de comando.

```
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;
    }
}
```

Os métodos de wrapper usados pelo cenário para as ações do registro de domínios do 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.";
        }
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API AWS SDK for .NET .
  - CheckDomainDisponibilidade
  - CheckDomainTransferibilidade
  - GetDomainDetalhe
  - GetDomainSugestões
  - GetOperationDetalhe
  - ListDomains
  - ListOperations

- ListPrices
- RegisterDomain
- ViewBilling

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da 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);
        }
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API AWS SDK for Java 2.x .
  - CheckDomainDisponibilidade
  - CheckDomainTransferibilidade
  - GetDomainDetalhe
  - GetDomainSugestões
  - GetOperationDetalhe
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
/**
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}")
            }
    }
}
```

- Para obter detalhes da API, consulte os tópicos a seguir na Referência da API AWS SDK para Kotlin.
  - CheckDomainDisponibilidade
  - CheckDomainTransferibilidade
  - GetDomainDetalhe
  - GetDomainSugestões
  - GetOperationDetalhe
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando o Route 53 com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Segurança no Amazon Route 53

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para obter mais informações sobre os programas de conformidade aplicáveis ao Amazon Route 53, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Route 53. Os tópicos a seguir mostram como configurar o Route 53 para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos do Route 53.

Tópicos

Proteção de dados no Route 53

O modelo de responsabilidade compartilhada da AWS aplica-se à proteção de dados no Amazon Route 53. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da Conta da AWS e configure as contas de usuário individuais com o AWS IAM Identity Center ou o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão dos Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso também é válido para quando você trabalha com o Route 53 ou outros produtos da Serviços da AWS, usando o console, a API, a AWS CLI ou os SDKs da AWS. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo,

recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Proteção contra registros de delegação pendentes no Route 53

Com o Route 53, você pode rotear tráfego para um subdomínio criando registros NS. Quando esses registros de NS apontam para servidores de nomes do Route 53, espera-se que os servidores de nomes correspondam aos do conjunto de delegação de uma zona hospedada que é autoritativa para o subdomínio. Se esses registros de NS não estiverem apontando para os servidores de nomes corretos, isso expõe ao risco de um ataque para explorar e assumir o controle do subdomínio. Eles registros são chamados de registros de NS pendurados.

Por exemplo, quando uma zona hospedada do Route 53 para um subdomínio é excluída, seus registros de NS podem ficar pendurados no domínio principal. Quando isso acontece, um ataque pode sequestrar o subdomínio criando uma nova zona hospedada nos servidores de nomes da zona excluída. O Route 53 tenta evitar isso acompanhando os pares de conjuntos de delegação do subdomínio e não permitindo que novas zonas do subdomínio sejam criadas nesses servidores de nomes antes que você remova os registros NS pendurados.

Porém, registros de NS pendurados ainda podem ocorrer devido à configuração incorreta dos registros de NS. Para mitigar esse risco, recomendamos que você tome as seguintes precauções:

- Confira se os registros de NS apex da zona hospedada autoritativa do Route 53 do subdomínio correspondem ao conjunto de delegação da zona hospedada. Você pode encontrar o conjunto de delegação de uma zona hospedada usando o console do Route 53 ou a AWS CLI. Para obter mais informações, consulte Listar registros ou get-hosted-zone.
- Habilite a assinatura de DNSSEC para a zona hospedada do Route 53 hospedada. O DNSEC autentica que as respostas do DNS vêm da fonte autorizada, evitando eficazmente o risco. Para mais informações, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.
- Remova os servidores de nomes que não hospedam o subdomínio dos registros de NS do subdomínio na zona hospedada superior.

  - ou -

- Substitua os servidores de nomes pelos quatro servidores de nomes no conjunto de delegação da zona hospedada autoritativa do subdomínio do Route 53. Isso também reduz eficazmente o risco.

Exemplos

Nos exemplos a seguir, presumimos que você tenha um domínio superior, `parent-domain.com`, e um subdomínio, `sub-domain.parent-domain.com`, mostramos três cenários em que há registros de NS pendurados e como reduzir o risco.

Cenário 1:

Na zona hospedada superior `parent-domain.com`, você cria registros de NS para `sub-domain.parent-domain.com` com quatro servidores de nomes <ns1>, <ns2>, <ns3> e <ns4>. E os servidores de nomes do subdomínio autoritativo são <ns5>, <ns6>, <ns7> e <ns8>. Assim sendo, <ns1>, <ns2>, <ns3> e <ns4> são todos registros de NS pendurados e isso expõe ao risco de que um ataque para obter o controle de subdomain.parent-domain.com. Para reduzir o risco, substitua o registro de NS do subdomínio por <ns5>, <ns6>, <ns7> e <ns8>.

Cenário 2:

`parent-domain.com` tem pontos de registros de NS `sub-domain.parent-domain.com` em <ns1>, <ns2>, <ns3>, <ns4>, <ns5>, <ns6>, <ns7> e <ns8>. E os servidores de nomes da zona hospedada do subdomínio autoritativo são <ns5>, <ns6>, <ns7> e <s8>. Assim sendo, <ns1>, <ns2>, <ns3> e <ns4> são novamente registros de NS pendurados. Para reduzir o risco, remova <ns1>, <ns2>, <ns3> e <ns4> dos registros de NS.

Cenário 3:

Você tem um conjunto de delegação reutilizável <ns1>, <ns2>, <ns3> e <ns4>. Você cria um registro de NS na zona superior e delega o subdomínio a esses servidores de nomes no conjunto de delegação reutilizável. Porém, você não criou a zona de subdomínio no conjunto de delegação reutilizável. Assim sendo, <ns1>, <ns2>, <ns3> e <ns4> são registros de NS pendurados. Para reduzir o risco, crie a zona hospedada do subdomínio com o conjunto de delegação reutilizável.

Gerenciamento de identidade e acesso no Amazon Route 53

Para realizar qualquer operação nos recursos do Amazon Route 53, como registrar um domínio ou atualizar um registro, o AWS Identity and Access Management (IAM) exige que você autentique que é um usuário aprovado AWS . Se estiver usando o console do Route 53, autentique sua identidade fornecendo seu nome de usuário e senha da AWS .

Depois de autenticar sua identidade, o IAM controla seu acesso ao AWS verificando se você tem permissões para realizar operações e acessar recursos. Se você for o administrador da conta,

poderá usar o IAM para controlar o acesso de outros usuários aos recursos que estão associados à sua conta.

Este capítulo explica como usar o IAM e o Route 53 para ajudar a proteger seus recursos.

Tópicos

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações

usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity Center Guia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity Center Manual do Usuário do.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne Chaves de Acesso Regularmente para Casos de Uso que exijam Credenciais de Longo Prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um nome de grupo IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após

a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no AWS IAM Identity Center Manual do Usuário.

- Permissões de usuários temporárias do IAM: um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as Funções do IAM Diferem das Políticas Baseadas em Recurso no Guia do Usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de Serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Controle de acesso

Para criar, atualizar, excluir ou indicar recursos do Amazon Route 53, você precisa de permissões para executar a operação e para acessar os recursos correspondentes.

As seções a seguir descrevem como gerenciar permissões para o Route 53. Recomendamos que você leia a visão geral primeiro.

Visão geral do gerenciamento de permissões de acesso aos recursos do Amazon Route 53

Cada AWS recurso pertence a uma AWS conta, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões.

> **Note**
>
> Administrador de conta (ou usuário administrador) é um usuário com privilégios correspondentes. Para obter mais informações sobre administradores, consulte Práticas recomendadas do IAM no Manual do usuário do IAM.

Ao conceder permissões, você decide quem recebe as permissões, os recursos relacionados às permissões concedidas e as ações que eles podem executar.

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas.
IAM	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs e ferramentas, consulte Autenticar usando credencia

Qual usuário precisa de acesso programático?	Para	Por
		is de longo prazo no Guia de referência de AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Tópicos

- ARNs para recursos do Amazon Route 53
- Informações sobre propriedade de recursos
- Gerenciamento de acesso aos recursos
- Especificar os elementos da política: recursos, ações, efeitos e principais
- Especificar condições em uma política

ARNs para recursos do Amazon Route 53

O Amazon Route 53 oferece suporte a diversos tipos de recursos para DNS, verificação de integridade e registro de domínio. Em uma política, você pode conceder ou negar acesso aos seguintes recursos usando * para o ARN:

- Verificações de integridade
- Zonas hospedadas
- Conjuntos de delegações reutilizáveis
- Status de um lote de alterações de conjunto de registros de recursos (somente API)
- Políticas de tráfego (fluxo de tráfego)
- Instâncias de política de tráfego (fluxo de tráfego)

Nem todos os recursos do Route 53 oferecem suporte a permissões. Você não pode conceder ou negar acesso aos seguintes recursos:

- Domínios
- Registros individuais
- Tags para domínios
- Tags para verificações de integridade
- Tags para zonas hospedadas

O Route 53 fornece ações de API para trabalhar com cada um desses tipos de recurso. Para obter mais informações, consulte Referência de API do Amazon Route 53. Para visualizar uma lista de ações e ARNs que podem ser especificadas para conceder ou negar permissão para usar cada ação, consulte Permissões da API do Amazon Route 53: referência de ações, recursos e condições.

Informações sobre propriedade de recursos

Uma AWS conta possui os recursos que são criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário do recurso é a AWS conta da entidade principal (ou seja, a conta raiz ou uma função do IAM) que autentica a solicitação de criação do recurso.

Os seguintes exemplos mostram como isso funciona:

- Se você usar as credenciais da conta raiz da sua AWS conta para criar uma zona hospedada, sua AWS conta é a proprietária do recurso.
- Se você criar um usuário em sua AWS conta e conceder permissões para criar uma zona hospedada para esse usuário, o usuário poderá criar uma zona hospedada. No entanto, a conta da AWS à qual o usuário pertence é proprietária do recurso da zona hospedada.
- Se você criar uma função do IAM em sua AWS conta com permissões para criar uma zona hospedada, qualquer pessoa que possa assumir a função poderá criar uma zona hospedada. Sua AWS conta, à qual a função pertence, é proprietária do recurso de zona hospedada.

Gerenciamento de acesso aos recursos

Uma política de permissões especifica quem tem acesso a quê. Esta seção explica as opções para criar políticas de permissões do Amazon Route 53. Para obter informações gerais sobre a sintaxe e as descrições de política do IAM, consulte a Referência da política do AWS IAM no Guia do usuário do IAM.

As políticas associadas a uma identidade do IAM são conhecidas como políticas baseadas em identidade (políticas do IAM) e as políticas associadas a um recurso são conhecidas como políticas

baseadas em recurso. O Route 53 oferece suporte apenas às políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em identidade (políticas do IAM)
- Políticas baseadas em recursos

Políticas baseadas em identidade (políticas do IAM)

Você pode anexar políticas a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexar uma política de permissões a um usuário ou grupo na sua conta: um administrador de conta pode usar uma política de permissões associada a um determinado usuário para conceder permissões para que esse usuário crie recursos do Amazon Route 53.
- Anexe uma política de permissões a uma função (conceda permissões entre contas) — Você pode conceder permissão para realizar ações do Route 53 a um usuário que foi criado por outra AWS conta. Para fazer isso, anexe uma política de permissões a uma função do IAM e permita que o usuário da outra conta assuma a função. O exemplo a seguir explica como isso funciona para duas contas da AWS , conta A e conta B:
  1. O administrador da conta A cria uma função do IAM e anexa à função uma política de permissões que concede permissões para criar ou acessar recursos de propriedade da conta A.
  2. O administrador da conta A associa uma política de confiança à função. A política de confiança identifica a conta B como a principal que pode assumir a função.
  3. O administrador da conta B pode delegar permissões para assumir a função para usuários ou grupos na conta B. Isso permite que os usuários na conta B criem ou acessem recursos na conta A.

  Para obter mais informações sobre como delegar permissões a usuários em outra AWS conta, consulte Gerenciamento de acesso no Guia do usuário do IAM.

A política de exemplo a seguir permite que um usuário execute a ação `CreateHostedZone` para criar uma zona hospedada pública para qualquer conta da AWS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Para que a política também se aplique a zonas hospedadas privadas, você precisa conceder permissões para usar a ação `AssociateVPCWithHostedZone` do Route 53 e duas ações do Amazon EC2, `DescribeVpcs` e `DescribeRegion`, conforme mostrado no exemplo a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeRegion"
            ],
            "Resource":"*"
        },
    ]
}
```

Para obter mais informações sobre como associar políticas a identidades para o Route 53, consulte Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Route 53. Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identidades (usuários, grupos e funções) no Manual do usuário do IAM.

Políticas baseadas em recursos

Outros produtos, como o Amazon S3, também permitem a anexação de políticas de permissões aos recursos. Por exemplo: você pode anexar uma política a um bucket do S3 para gerenciar permissões de acesso a esse bucket. O Amazon Route 53 não oferece suporte para anexar políticas a recursos.

Especificar os elementos da política: recursos, ações, efeitos e principais

O Amazon Route 53 inclui ações de API (consulte a Referência de API do Amazon Route 53) que você pode usar em cada recurso do Route 53 (consulte ARNs para recursos do Amazon Route 53). Você pode conceder a um usuário ou a um usuário federado permissões para executar uma ou todas essas ações. Observe que algumas ações de API, como registrar um domínio, exigem permissões para executar mais de uma ação.

Estes são os elementos de política básicos:

- Recurso: use um nome de recurso da Amazon (ARN) para identificar o recurso ao qual a política se aplica. Para obter mais informações, consulte ARNs para recursos do Amazon Route 53.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que você deseja permitir ou negar. Por exemplo, dependendo do `Effect` especificado, a permissão `route53:CreateHostedZone` permite ou nega a um usuário a capacidade de executar a ação `CreateHostedZone` do Route 53.
- Efeito: você especifica o efeito, permitir ou negar, quando um usuário tenta executar a ação no recurso especificado. Se você não conceder acesso explícito a uma ação, o acesso será negado implicitamente. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (isso se aplica somente a políticas baseadas em recursos). O Route 53 não é compatível com políticas baseadas em recursos.

Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte Referência da política do AWS IAM no Guia do usuário do IAM.

Para obter uma em tabela mostrando todas as operações da API do Route 53 e os recursos aos quais elas se aplicam, consulte Permissões da API do Amazon Route 53: referência de ações, recursos e condições.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar quando uma política deve entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política de acesso, consulte Elementos de política do IAM JSON: condição no Manual do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do Route 53. No entanto, existem chaves AWS de condição amplas que você pode usar conforme necessário. Para obter uma lista completa de chaves AWS largas, consulte Chaves disponíveis para condições no Guia do usuário do IAM.

Usar políticas baseadas em identidade (políticas do IAM) para o Amazon Route 53

Este tópico fornece exemplos de políticas baseadas em identidade que demonstram como um administrador de conta pode anexar políticas de permissões a identidades do IAM e, dessa forma, conceder permissões para executar operações em recursos do Amazon Route 53.

Important

Recomendamos que você analise primeiramente os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos recursos do Route 53. Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos recursos do Amazon Route 53.

Note

Ao conceder acesso, a zona hospedada e a Amazon VPC devem pertencer à mesma partição. Uma partição é um grupo de Regiões da AWS. Cada uma Conta da AWS tem como escopo uma partição.
Estas são as partições compatíveis:

- `aws` - Regiões da AWS
- `aws-cn`: regiões da China
- `aws-us-gov` - AWS GovCloud (US) Region

Para obter mais informações, consulte Gerenciamento de acesso e Cotas e endpoints do Amazon Route 53 na Referência geral da AWS .

Tópicos

- Permissões necessárias para usar o console do Amazon Route 53
- Permissões de exemplo para um proprietário de registro de domínio
- Permissões de chave gerenciada pelo cliente do Route 53 necessárias para assinatura DNSSEC
- Exemplos de política gerenciada pelo cliente

A seguir, um exemplo de uma política de permissões. O `Sid`, ou o ID de instrução, é opcional:

```
{
    "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": "*"
        }
    ]
}
```

A política inclui duas instruções:

- A primeira instrução concede permissões para as ações necessárias para criar e gerenciar zonas hospedadas públicas e seus registros. O caractere curinga (*) no Amazon Resource Name (ARN) concede acesso a todas as zonas hospedadas que pertencem à AWS conta atual.
- A segunda instrução concede permissões para todas as ações necessárias para criar e gerenciar verificações de integridade.

Para visualizar uma lista de ações e ARNs que podem ser especificadas para conceder ou negar permissão para usar cada ação, consulte Permissões da API do Amazon Route 53: referência de ações, recursos e condições.

Permissões necessárias para usar o console do Amazon Route 53

Para conceder acesso total ao console do Amazon Route 53, conceda as permissões na seguinte política de permissões:

```
{
    "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"
        }
    ]
}
```

Veja por que as permissões são necessárias:

`route53:*`

Permite que você execute todas as ações do Route 53, com exceção das seguintes:

- Crie e atualize registros de alias para os quais o valor de Alias Target seja uma CloudFront distribuição, um balanceador de carga do Elastic Load Balancing, um ambiente do Elastic

Beanstalk ou um bucket do Amazon S3. (Com essas permissões, você pode criar registros de alias para os quais o valor de Alvo do alias é outro registro na mesma zona hospedada.)

- Como trabalhar com zonas hospedadas privadas.
- Trabalhando com domínios.
- Crie, exclua e visualize CloudWatch alarmes.
- CloudWatch Métricas de renderização no console do Route 53.

`route53domains:*`

Permite que você trabalhe com domínios.

> **Important**
>
> Se você relacionar as ações `route53` individualmente, deverá incluir `route53:CreateHostedZone` para trabalhar com domínios. Quando você registra um domínio, uma zona hospedada é criada ao mesmo tempo. Portanto, uma política que inclui permissões para registrar domínios também requer permissão para criar zonas hospedadas.

Para o registro de domínio, o Route 53 não oferece suporte à concessão ou negação de permissões para recursos individuais.

`route53resolver:*`

Permite que você trabalhe com o Route 53 Resolver.

`ssm:GetParametersByPath`

Permite que você busque regiões disponíveis publicamente ao criar novos registros de alias, zonas hospedadas privadas e verificações de integridade.

`cloudfront:ListDistributions`

Permite criar e atualizar registros de alias para os quais o valor de Alias Target é uma CloudFront distribuição.

Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 utiliza-o apenas para obter uma lista de distribuições para exibir no console.

`elasticloadbalancing:DescribeLoadBalancers`

Permite que você crie e atualize registros de alias para os quais o valor de Alvo do alias é um load balancer do ELB.

Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de balanceadores de carga para exibir no console.

`elasticbeanstalk:DescribeEnvironments`

Permite que você crie e atualize registros com alias para os quais o valor de Alias Target (Destino do alias) é um ambiente do Elastic Beanstalk.

Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de ambientes para exibir no console.

`s3:ListAllMyBuckets`, **`s3:GetBucketLocation`**, e **`s3:GetBucketWebsite`**

Permite que você crie e atualize registros com alias para os quais o valor de Alias Target (Destino do alias) é um bucket do Amazon S3. (Você só poderá criar um alias para um bucket do Amazon S3 se o bucket estiver configurado como um endpoint do site. `s3:GetBucketWebsite` obtém as informações de configuração necessárias.)

Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 utiliza-o apenas para obter uma lista de buckets para exibir no console.

`ec2:DescribeVpcs` e **`ec2:DescribeRegions`**

Permite que você trabalhe com zonas hospedadas privadas.

Todas as permissões **`ec2`** listadas

Permite que você trabalhe com o Route 53 Resolver.

`sns:ListTopics`, **`sns:ListSubscriptionsByTopic`**, **`sns:CreateTopic`**, **`cloudwatch:DescribeAlarms`**, **`cloudwatch:PutMetricAlarm`**, **`cloudwatch:DeleteAlarms`**

Permite criar, excluir e visualizar CloudWatch alarmes.

`cloudwatch:GetMetricStatistics`

Permite criar verificações CloudWatch métricas de integridade.

Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter as estatísticas a serem exibidas no console.

`apigateway:GET`

Permite que você crie e atualize registros de alias para os quais o valor de Alias Target (Destino do alias) é uma API do Amazon API Gateway.

Essa permissão não é necessária se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de APIs para exibir no console.

`kms:*`

Permite que você trabalhe AWS KMS para habilitar a assinatura do DNSSEC.

Permissões de exemplo para um proprietário de registro de domínio

Com as permissões do conjunto de registros de recursos, você pode definir permissões granulares que limitam o que o AWS usuário pode atualizar ou modificar. Para ter mais informações, consulte Uso de condições de política do IAM para controle de acesso refinado para gerenciar conjuntos de registros de recursos.

Em alguns cenários, um proprietário de zona hospedada pode ser responsável pelo gerenciamento geral da zona hospedada, enquanto outra pessoa na organização é responsável por um subconjunto dessas tarefas. Um proprietário de zona hospedada que habilitou a assinatura DNSSEC, por exemplo, pode querer criar uma política do IAM que inclua a permissão para outra pessoa adicionar e excluir registros de conjunto de recursos (RRs) na zona hospedada, entre outras tarefas. As permissões específicas que um proprietário de zona hospedada escolhe habilitar para um proprietário de registro ou outras pessoas dependerão da política de sua organização.

Veja a seguir um exemplo de política do IAM que permite que um proprietário de registro faça modificações em RRs, políticas de tráfego e verificações de integridade. Um proprietário de registro com essa política não tem permissão para realizar operações em nível de região, como criar ou excluir uma zona, habilitar ou desabilitar o log de consultas, criar ou excluir um conjunto de delegações reutilizáveis ou alterar configurações de 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": [
        "*"
      ]
}
```

Permissões de chave gerenciada pelo cliente do Route 53 necessárias para assinatura DNSSEC

Quando você ativa a assinatura do DNSSEC para o Route 53, o Route 53 cria uma chave de assinatura de chave (KSK) com base em uma chave gerenciada pelo cliente em (). AWS Key Management Service AWS KMS Você pode usar uma chave gerenciada pelo cliente existente que suporte a assinatura de DNSSEC ou criar uma nova. O Route 53 deve ter permissão para acessar sua chave gerenciada pelo cliente para que ele possa criar o KSK para você.

Para habilitar o Route 53 para acessar sua chave gerenciada pelo cliente, verifique se a diretiva de chave gerenciada pelo cliente contém as seguintes instruções:

```
{
            "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
                }
            }
        }
```

O problema de representante confuso é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Para se AWS KMS proteger disso, você pode, opcionalmente, limitar as permissões que um serviço tem para um recurso em uma política baseada em recursos fornecendo uma combinação de `aws:SourceAccount` `aws:SourceArn` condições (ambas ou uma). `aws:SourceAccount`é o ID da AWS conta de um proprietário de uma zona hospedada. `aws:SourceArn`é um ARN de uma zona hospedada.

Veja a seguir dois exemplos de permissões que podem ser adicionadas:

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

- Ou -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
```

```
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

Para obter mais informações, consulte O problema confused deputy no Guia do usuário IAM.

Exemplos de política gerenciada pelo cliente

Você pode criar suas próprias políticas personalizadas do IAM para conceder permissões para ações do Route 53. Você pode anexar essas políticas personalizadas a grupos do IAM que exijam as permissões especificadas. Essas políticas funcionam quando você está usando a API do Route 53, os AWS SDKs ou a AWS CLI. Os exemplos a seguir mostram permissões para vários casos de uso comuns. Para a política que concede acesso total de um usuário ao Route 53, consulte Permissões necessárias para usar o console do Amazon Route 53.

Exemplos

- Exemplo 1: permitir acesso de leitura a todas as zonas hospedadas
- Exemplo 2: permitir criação e exclusão de zonas hospedadas
- Exemplo 3: permitir acesso total a todos os domínios (somente zonas hospedadas públicas)
- Exemplo 4: permitir a criação de endpoints de entrada e saída do Route 53 Resolver

Exemplo 1: permitir acesso de leitura a todas as zonas hospedadas

A política de permissões a seguir concede as permissões de usuário para listar todas as zonas hospedadas e visualizar todos os registros em uma zona hospedada.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
```

```
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

Exemplo 2: permitir criação e exclusão de zonas hospedadas

A política de permissões a seguir permite que os usuários criem e excluam zonas hospedadas assim como acompanhem o andamento da alteração.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

Exemplo 3: permitir acesso total a todos os domínios (somente zonas hospedadas públicas)

A política de permissões a seguir permite que os usuários executem todas as ações em registros de domínio, incluindo permissões para registrar domínios e criar zonas hospedadas.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

Quando você registra um domínio, uma zona hospedada é criada ao mesmo tempo. Assim, uma política que inclui permissões para registrar domínios também requer permissões para criar zonas hospedadas. (Para o registro de domínio, o Route 53 não oferece suporte à concessão de permissões para recursos individuais.)

Para obter informações sobre permissões necessárias para trabalhar com zonas hospedadas privadas, consulte Permissões necessárias para usar o console do Amazon Route 53.

Exemplo 4: permitir a criação de endpoints de entrada e saída do Route 53 Resolver

A política de permissões a seguir permite que os usuários usem o console do Route 53 para criar endpoints de entrada e saída do Resolver.

Algumas dessas permissões são necessárias apenas para criar endpoints no console. Você pode omitir essas permissões se desejar conceder permissões somente para criar endpoints de entrada e saída de forma programática:

- `route53resolver:ListResolverEndpoints` permite que os usuários vejam a lista de endpoints de entrada ou saída para que possam verificar se um endpoint foi criado.
- `DescribeAvailabilityZones` é necessário para exibir uma lista de zonas de disponibilidade.
- `DescribeVpcs` é necessário para exibir uma lista de 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": "*"
        }
    ]
}
```

Usar funções vinculadas ao serviço do Amazon Route 53 Resolver

O Route 53 Resolver usa funções vinculadas ao produto do AWS Identity and Access Management (IAM). A função vinculada ao produto é um tipo exclusivo de função do IAM vinculada diretamente ao Resolver. As funções vinculadas a produtos são predefinidas pelo Resolver e incluem todas as permissões que o produto requer para chamar outros produtos da AWS em seu nome.

Uma função vinculada ao produto facilita a configuração do Resolver porque você não precisa adicionar as permissões necessárias manualmente. O Resolver define as permissões das funções vinculadas ao produto e, exceto se definido de outra forma, somente o Resolver pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir uma função vinculada ao serviço somente depois de excluir os recursos relacionados da Isso protege seus recursos do Resolver, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte o tópico sobre Serviços da AWS compatíveis com o IAM e procure serviços que tenham Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Tópicos

- Permissões de função vinculada ao produto do Resolver
- Criar uma função vinculada ao produto para o Resolver
- Como editar uma função vinculada ao produto para o Resolver
- Como excluir uma função vinculada ao produto do Resolver
- Regiões com suporte a funções vinculadas a produto do Resolver

Permissões de função vinculada ao produto do Resolver

O Resolver usa a função vinculada ao produto da **`AWSServiceRoleForRoute53Resolver`** para entregar logs de consulta em seu nome.

A política de permissões da função permite que o Resolver conclua as seguintes ações em todos os recursos:

```
{
  "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": "*"
    }
  ]
}
```

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Criar uma função vinculada ao produto para o Resolver

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria uma associação de configuração de log de consulta do resolvedor no console do Amazon Route 53, a AWS CLI, ou o API da AWS, o Resolver cria uma função vinculada ao produto para você.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos compatíveis com essa função. Além disso, se você estava usando o produto do Resolver antes de 12 de agosto de 2020 quando ele começou a oferecer suporte às funções vinculadas ao produto, o Resolver criou a função `AWSServiceRoleForRoute53Resolver` em sua conta. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria uma associação de configuração de log de consulta do Resolver, a função vinculada ao produto do `AWSServiceRoleForRoute53Resolver` é criada para você novamente.

Como editar uma função vinculada ao produto para o Resolver

O Resolver não permite que você edite a função vinculada ao produto `AWSServiceRoleForRoute53Resolver`. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

Como excluir uma função vinculada ao produto do Resolver

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o produto do Resolver estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do Resolver usados pelo **`AWSServiceRoleForRoute53Resolver`**

1. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Expanda o menu do console do Route 53. No canto superior esquerdo do console, escolha o ícone de três barras horizontais ().
3. No menu do Resolver, escolha Query logging (Log de consultas).
4. Marque a caixa de seleção ao lado do nome da configuração do log de consultas e escolha Delete (Excluir).
5. Na caixa de texto Delete query logging configuration (Excluir configuração de log de consultas), selecione Stop logging queries (Interromper consultas de log).

   Isso desassociará a configuração da VPC. Você também pode desassociar a configuração de log de consulta de forma programada. Para obter mais informações, consulte disassociate-resolver-query-log-config.
6. Depois que as consultas de log forem interrompidas, você poderá digitar opcionalmente **`delete`** no campo e escolher Delete (Excluir) para excluir a configuração do log de consultas. No entanto, isso não é necessário para excluir os recursos usados pelo `AWSServiceRoleForRoute53Resolver`.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço `AWSServiceRoleForRoute53Resolver`. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas a produto do Resolver

O Resolver não oferece suporte ao uso de funções vinculadas a produtos em todas as regiões em que o produto está disponível. Você pode usar a função `AWSServiceRoleForRoute53Resolver` nas seguintes regiões.

Nome da região	Identidade da região	Suporte no Resolver
Leste dos EUA (N. da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
Oeste dos EUA (N. da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
Ásia-Pacífico (Mumbai)	ap-south-1	Sim
Asia Pacific (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim
Europa (Paris)	eu-west-3	Sim
América do Sul (São Paulo)	sa-east-1	Sim
China (Pequim)	cn-north-1	Sim

Nome da região	Identidade da região	Suporte no Resolver
China (Ningxia)	cn-northwest-1	Sim
AWS GovCloud (US)	us-gov-east-1	Sim
AWS GovCloud (US)	us-gov-west-1	Sim

AWS políticas gerenciadas para o Amazon Route 53

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AmazonRoute 53 FullAccess

É possível anexar a política `AmazonRoute53FullAccess` a suas identidades do IAM.

Esta política concede acesso total a recursos do Route 53, incluindo registro de domínio e verificação de integridade, mas excluindo o Resolver.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53:*`: permite que você execute todas as ações do Route 53 com exceção das seguintes:

  - Crie e atualize registros de alias para os quais o valor de Alias Target seja uma CloudFront distribuição, um balanceador de carga do Elastic Load Balancing, um ambiente do Elastic Beanstalk ou um bucket do Amazon S3. (Com essas permissões, você pode criar registros de alias para os quais o valor de Alvo do alias é outro registro na mesma zona hospedada.)
  - Como trabalhar com zonas hospedadas privadas.
  - Trabalhando com domínios.
  - Crie, exclua e visualize CloudWatch alarmes.
  - Renderize CloudWatch métricas no console do Route 53.
- `route53domains:*`: permite que você trabalhe com domínios.
- `cloudfront:ListDistributions`— Permite criar e atualizar registros de alias para os quais o valor de Alias Target é uma CloudFront distribuição.

  Esta permissão não é necessária se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de distribuições para exibir no console.
- `elasticloadbalancing:DescribeLoadBalancers`: permite que você crie e atualize registros de alias para os quais o valor de Alias Target (Destino do alias) é um balanceador de carga do Elastic Load Balancing.

  Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de balanceadores de carga para exibir no console.
- `elasticbeanstalk:DescribeEnvironments`: permite que você crie e atualize registros com alias para os quais o valor de Alias Target (Destino do alias) é um ambiente do Elastic Beanstalk.

  Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de ambientes para exibir no console.
- `s3:ListBucket`, `s3:GetBucketLocation` e `s3:GetBucketWebsite`: permite que você crie e atualize registros com alias para os quais o valor de Alias Target (Destino do alias) é um bucket do Amazon S3. (Você só poderá criar um alias para um bucket do Amazon S3 se o bucket estiver configurado como um endpoint do site. `s3:GetBucketWebsite` obtém as informações de configuração necessárias.)

  Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 as utiliza apenas para obter uma lista de buckets para exibir no console.
- `ec2:DescribeVpcs`: permite que você exiba uma lista de VPCs.
- `ec2:DescribeVpcEndpoints`: permite exibir uma lista de endpoints da VPC.

- `ec2:DescribeRegions`: permite que você exiba uma lista de zonas de disponibilidade.
- `sns:ListTopics`,`sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` — Permite criar, excluir e visualizar CloudWatch alarmes.
- `cloudwatch:GetMetricStatistics`— Permite criar verificações CloudWatch métricas de integridade.

  Essas permissões não são necessárias se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter as estatísticas a serem exibidas no console.
- `apigateway:GET`: permite que você crie e atualize registros de alias para os quais o valor de Alias Target (Destino do alias) é uma API do Amazon API Gateway.

  Essa permissão não é necessária se você não estiver usando o console do Route 53. O Route 53 usa-o apenas para obter uma lista de APIs para exibir no console.

Para obter mais informações sobre as permissões, consulte[Permissões da API do Amazon Route 53: referência de ações, recursos e condições](#).

```
{
    "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 política gerenciada: AmazonRoute 53 ReadOnlyAccess

É possível anexar a política `AmazonRoute53ReadOnlyAccess` a suas identidades do IAM.

Esta política concede acesso somente para leitura aos recursos do Route 53, incluindo registro de domínio e verificação de integridade, mas excluindo o Resolver.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53:Get*`: obtém os recursos do Route 53.
- `route53:List*`: lista os recursos do Route 53.
- `route53:TestDNSAnswer`: obtém o valor que o Route 53 retorna em resposta a uma solicitação de DNS.

Para obter mais informações sobre as permissões, consulte Permissões da API do Amazon Route 53: referência de ações, recursos e condições.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
```

```
        }
    ]
}
```

AWS política gerenciada: AmazonRoute 53 DomainsFullAccess

É possível anexar a política `AmazonRoute53DomainsFullAccess` a suas identidades do IAM.

Esta política concede acesso total aos recursos de registro de domínio do Route 53.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53:CreateHostedZone`: permite que você crie uma zona hospedada do Route 53.
- `route53domains:*`: permite registrar nomes de domínio e executar operações relacionadas.

Para obter mais informações sobre as permissões, consulte[Permissões da API do Amazon Route 53: referência de ações, recursos e condições](#).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS política gerenciada: AmazonRoute 53 DomainsReadOnlyAccess

É possível anexar a política `AmazonRoute53DomainsReadOnlyAccess` a suas identidades do IAM.

Esta política concede acesso somente leitura a recursos de registro de domínio do Route 53.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53domains:Get*`: permite recuperar uma lista de domínios do Route 53.
- `route53domains:List*`: permite exibir uma lista de domínios do Route 53.

Para obter mais informações sobre as permissões, consultePermissões da API do Amazon Route 53: referência de ações, recursos e condições.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS política gerenciada: AmazonRoute 53 ResolverFullAccess

É possível anexar a política `AmazonRoute53ResolverFullAccess` a suas identidades do IAM.

Esta política concede acesso total aos recursos do Route 53 Resolver.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53resolver:*`: permite criar e gerenciar recursos do Resolver no console do Route 53.
- `ec2:DescribeSubnets`: permite que você liste suas sub-redes da Amazon VPC.

- `ec2:CreateNetworkInterface`,`ec2:DeleteNetworkInterface`, e `ec2:ModifyNetworkInterfaceAttribute`: permite criar, modificar e excluir interfaces de rede.
- `ec2:DescribeNetworkInterfaces`: permite que você exiba uma lista de interfaces de rede.
- `ec2:DescribeSecurityGroups`: permite que você exiba uma lista de todos os seus grupos de segurança.
- `ec2:DescribeVpcs`: permite que você exiba uma lista de VPCs.
- `ec2:DescribeAvailabilityZones`: permite listar as zonas que estão disponíveis para você.

Para obter mais informações sobre as permissões, consultePermissões da API do Amazon Route 53: referência de ações, recursos e condições.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS política gerenciada: AmazonRoute 53 ResolverReadOnlyAccess

É possível anexar a política `AmazonRoute53ResolverReadOnlyAccess` a suas identidades do IAM.

Esta política concede acesso somente leitura aos recursos do Route 53 Resolver.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `route53resolver:Get*`— Obtém recursos do Resolver.
- `route53resolver:List*`: permite que você exiba uma lista de recursos do Resolvedor.
- `ec2:DescribeNetworkInterfaces`: permite que você exiba uma lista de interfaces de rede.
- `ec2:DescribeSecurityGroups`: permite que você exiba uma lista de todos os seus grupos de segurança.

Para obter mais informações sobre as permissões, consulte[Permissões da API do Amazon Route 53: referência de ações, recursos e condições](#).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS política gerenciada: Route53 ResolverServiceRolePolicy

Não é possível anexar `Route53ResolverServiceRolePolicy` às entidades do IAM. Esta política é anexada a uma função vinculada ao produto que permite que o Route 53 Resolver acesse

os produtos e recursos da AWS que são usados ou gerenciados pelo Resolver. Para ter mais informações, consulte Usar funções vinculadas ao serviço do Amazon Route 53 Resolver.

AWS política gerenciada: AmazonRoute 53 ProfilesFullAccess

É possível anexar a política `AmazonRoute53ProfilesReadOnlyAccess` a suas identidades do IAM.

Essa política concede acesso total aos recursos do Amazon Route 53 Profile.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `ec2`— Permite que os diretores obtenham informações sobre VPCs.

Para obter mais informações sobre as permissões, consultePermissões da API do Amazon Route 53: referência de ações, recursos e condições.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
```

```
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS política gerenciada: AmazonRoute 53 ProfilesReadOnlyAccess

É possível anexar a política `AmazonRoute53ProfilesReadOnlyAccess` a suas identidades do IAM.

Essa política concede acesso somente para leitura aos recursos do Amazon Route 53 Profile.

Detalhes da permissão

Para obter mais informações sobre as permissões, consulte[Permissões da API do Amazon Route 53: referência de ações, recursos e condições](#).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
```

```
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Atualizações do Route 53 para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Route 53 desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Document history (Histórico de documentos) do Route 53.

Alteração	Descrição	Data
AmazonRoute53 ProfilesFullAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso total aos recursos do perfil do Amazon Route 53.	22 de abril de 2024
AmazonRoute53 ProfilesReadOnlyAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso somente de leitura aos recursos do perfil do Amazon Route 53.	22 de abril de 2024
Route53 ResolverServiceRolePolicy — Nova política	O Amazon Route 53 adicionou uma nova política anexada a uma função vinculada a serviços que permite que o Route 53 Resolver acesse AWS serviços e recursos que	14 de julho de 2021

Alteração	Descrição	Data
	são usados ou gerenciados pelo Resolver.	
AmazonRoute53 ResolverReadOnlyAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso somente de leitura aos recursos do Route 53 Resolver.	14 de julho de 2021
AmazonRoute53 ResolverFullAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso total aos recursos do Route 53 Resolver.	14 de julho de 2021
AmazonRoute53 DomainsReadOnlyAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso somente de leitura aos recursos de domínios do Route 53.	14 de julho de 2021
AmazonRoute53 DomainsFullAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso total aos recursos dos domínios do Route 53.	14 de julho de 2021
AmazonRoute53 ReadOnlyAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso somente de leitura aos recursos do Route 53.	14 de julho de 2021

Alteração	Descrição	Data
AmazonRoute53 FullAccess — Nova política	O Amazon Route 53 adicionou uma nova política para permitir acesso total aos recursos do Route 53.	14 de julho de 2021
O Route 53 começou a monitorar alterações	O Route 53 começou a monitorar as mudanças em suas políticas AWS gerenciadas.	14 de julho de 2021

Uso de condições de política do IAM para controle de acesso refinado para gerenciar conjuntos de registros de recursos

Ao conceder permissões nos conjuntos de registros de recursos no Route 53, você pode especificar as condições que determinam como uma política de permissões entra em vigor.

No Route 53, é possível especificar as condições ao conceder permissões usando uma política do IAM (consulte Controle de acesso). Por exemplo, é possível:

- Conceda permissões para liberar o acesso a um único conjunto de registros de recursos.
- Conceda permissões para liberar o acesso aos usuários a todos os conjuntos de registros de recursos de um tipo específico de registro DNS em uma zona hospedada, por exemplo, registros A e AAAA.
- Conceda permissões para liberar o acesso aos usuários a um conjunto de registros de recursos em que seu nome contém uma string específica.
- Conceda permissões para permitir que os usuários realizem somente um subconjunto das `CREATE | UPSERT | DELETE` ações no console do Route 53 ou ao usar a ChangeResourceRecordSetsAPI.

Você também pode criar permissões que combinam qualquer uma das permissões granulares.

Use o elemento `Condition` do IAM para implementar uma política de controle de acesso refinada. Ao adicionar um elemento `Condition` de uma política de permissões, você pode liberar ou negar o acesso a registros em conjuntos de registros de recursos do Route 53 com base em seus requisitos

comerciais. Por exemplo, sua política do IAM pode restringir o acesso a registros DNS individuais em uma zona hospedada. Você então poderá anexar a política a usuários, grupos ou perfis.

Como normalizar os valores-chave da condição

Os valores inseridos para as condições da política devem ser formatados ou normalizados da seguinte forma:

Para **`route53:ChangeResourceRecordSetsNormalizedRecordNames`**:

- Todas as letras devem estar em minúscula.
- O nome DNS deve estar sem o ponto final.
- Caracteres que não sejam de A a Z, 0 a 9, - (hífen), _ (underline) e . (ponto final, como delimitador entre rótulos) deve usar códigos de escape no formato \código octal de três dígitos. Por exemplo, `\052` é o código octal para o caractere *.

Para **`route53:ChangeResourceRecordSetsActions`**, o valor pode ser qualquer um dos seguintes e deve estar em maiúsculas:

- CREATE
- UPSERT
- DELETE

para **`route53:ChangeResourceRecordSetsRecordTypes`**:

- O valor deve estar em maiúsculas e pode ser qualquer um dos tipos de registro DNS compatíveis com o Route 53. Para ter mais informações, consulte Tipos de registro de DNS com suporte.

> **Important**
>
> Para que suas permissões liberem ou restrinjam as ações pretendidas, você deve seguir essas convenções.

Você pode usar o Access Analyzer ou Policy Simulator no Guia de usuário do IAM para validar que a política libera ou restringe as permissões conforme o esperado. Você também pode validar as

permissões aplicando uma política do IAM a um usuário ou função de teste para realizar operações do Route 53.

Especificar condições: usar chaves de condição

AWS fornece um conjunto de chaves de condição predefinidas (chaves AWS de condição abrangentes) para todos os AWS serviços que oferecem suporte ao IAM para controle de acesso. Por exemplo, você pode usar a condição de chave `aws:SourceIp` para verificar o endereço IP do solicitante antes de permitir que uma ação seja executada. Para obter mais informações e uma lista das chaves no âmbito da AWS, consulte Chaves disponíveis para condições no Guia do usuário do IAM.

> **Note**
>
> O Route 53 não é compatível com chaves de condição baseadas em tag.

A tabela a seguir mostra as chaves de condição específicas do serviço do Route 53 que se aplicam aos conjuntos de registros de recursos.

Chave de condição do Route 53	Operações de API	Tipo de valor	Descrição
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	Vários valores	Representa uma lista de nomes de registros DNS na solicitação de ChangeResourceRecordSets. Para obter o comportamento esperado, os nomes DNS na política do IAM devem ser normalizados da seguinte forma: • Todas as letras devem estar em minúscula. • O nome DNS deve estar sem o ponto final. • Caracteres que não sejam de A a Z, 0 a 9, - (hífen), _ (underline) e . (ponto final, como delimitador entre rótulos) deve usar códigos

Chave de condição do Route 53	Operações de API	Tipo de valor	Descrição
			de escape no formato \código octal de três dígitos.
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	Vários valores	Representa uma lista de tipos de registro DNS na solicitação de `ChangeResourceRecordSets` . `ChangeResourceRecordSetsRecordTypes` pode ser qualquer um dos tipos de registro DNS compatíveis com o Route 53. Para ter mais informações, consulte Tipos de registro de DNS com suporte. Todos devem ser inseridos em maiúsculas na política.
`route53:ChangeResourceRecordSetsActions`	ChangeResourceRecordSets	Vários valores	Representa uma lista de ações na solicitação de `ChangeResourceRecordSets` . `ChangeResourceRecordSetsActions` pode ser qualquer um dos seguintes valores (deve estar em maiúsculas): • CREATE • UPSERT • DELETE

Políticas de exemplo: usar condições para acesso refinado

Cada um dos exemplos nessa seção define a cláusula Effect (Efeito) como Allow (Permitir) e especifica apenas as ações, os recursos e os parâmetros permitidos. O acesso é permitido apenas para o que está listado explicitamente na política do IAM.

Em alguns casos, é possível reescrever essas políticas para que elas sejam baseadas em negação (ou seja, definindo a cláusula Effect (Efeito) como Deny (Negar) e invertendo toda a lógica na política). No entanto, recomendamos que você evite usar políticas baseadas em negação, pois elas são difíceis de escrever corretamente, em comparação às políticas baseadas em permissão. Pela necessidade de normalização do texto, isso é especialmente verdadeiro para o Route 53.

Conceder permissões que limitam o acesso a registros DNS com nomes específicos

A política de permissões a seguir concede permissões para as ações `ChangeResourceRecordSets` na zona hospedada Z12345 para exemplo.com e marketing.exemplo.com. Ele usa a chave de condição `route53:ChangeResourceRecordSetsNormalizedRecordNames` para limitar as ações do usuário somente nos registros que correspondem aos nomes especificados.

```
{
    "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` é um operador de condição do IAM que se aplica a chaves de vários valores. A condição na política acima permitirá a operação somente quando todas as alterações em `ChangeResourceRecordSets` tenham o nome DNS de example.com. Para obter mais informações, consulte Operadores de condição do IAM e Condição do IAM com várias chaves ou valores no Guia do usuário do IAM.

Para implementar a permissão que combina nomes com determinados sufixos, você pode usar o coringa do IAM (*) na política com operador de condição `StringLike` ou `StringNotLike`. A política a seguir permitirá a operação quando todas as alterações na operação `ChangeResourceRecordSets` tiverem nomes DNS que terminam com “-beta.example.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**
>
> O coringa do IAM não é o mesmo que o coringa do nome de domínio. Veja o exemplo a seguir para saber como usar o coringa com um nome de domínio.

Conceda permissões que limitam o acesso aos registros DNS que correspondem a um nome de domínio contendo um coringa

A política de permissões a seguir concede permissões que possibilitam ações `ChangeResourceRecordSets` na zona hospedada Z12345 para example.com. Ele usa a chave de condição `route53:ChangeResourceRecordSetsNormalizedRecordNames` para limitar as ações do usuário somente aos registros que correspondam a *.example.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 é o código octal para o caractere * no nome DNS e \ em \052 escapou para ser \\ para seguir a sintaxe JSON.

Conceder permissões que limitam o acesso a determinados registros DNS

A política de permissões a seguir concede permissões que possibilitam ações ChangeResourceRecordSets na zona hospedada Z12345 para example.com. Ele usa a combinação de três chaves de condição para limitar as ações do usuário e permitir somente a criação ou edição de registros DNS com determinado nome e tipo de 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"]
                }
            }
          }
        ]
}
```

Conceder permissões que limitam o acesso à criação e edição apenas dos tipos especificados de registros DNS

A política de permissões a seguir concede permissões que possibilitam ações ChangeResourceRecordSets na zona hospedada Z12345 para example.com. Ele usa a chave de

condição `route53:ChangeResourceRecordSetsRecordTypes` para limitar as ações do usuário somente nos registros que correspondem aos tipos especificados (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"]
                }
            }
          }
        ]
}
```

Permissões da API do Amazon Route 53: referência de ações, recursos e condições

Ao configurar Controle de acesso e escrever uma política de permissões que você pode anexar a uma identidade do IAM (políticas baseadas em identidade), você pode usar as listas de ações, recursos e chaves de condição para o Route 53, ações, recursos e chaves de condição para domínios do Route 53, ações, recursos e chaves de condição para o Route 53 Resolver, e ações, recursos e chaves de condição para perfis do Amazon Route 53 permitem compartilhar configurações de DNS com VPCs na Referência de autorização de serviço. As páginas incluem cada ação da API do Amazon Route 53, as ações às quais você deve conceder permissões de acesso e o AWS recurso ao qual você deve conceder acesso. Você especifica as ações no campo `Action` da política e o valor do recurso no campo `Resource` da política.

Você pode usar chaves de condição AWS-wide em suas políticas do Route 53 para expressar condições. Para obter uma lista completa AWS de chaves gerais, consulte Chaves disponíveis no Guia do usuário do IAM.

> **Note**
>
> Ao conceder acesso, a zona hospedada e a Amazon VPC devem pertencer à mesma partição. Uma partição é um grupo de Regiões da AWS. Cada uma Conta da AWS tem como escopo uma partição.
> Estas são as partições compatíveis:
>
> - `aws` - Regiões da AWS
> - `aws-cn`: regiões da China
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> Para obter mais informações, consulte Gerenciamento de acesso em Referência geral da AWS .

> **Note**
>
> Para especificar uma ação, use o prefixo aplicável (`route53`, `route53domains` ou `route53resolver`) seguido do nome de operação da API, por exemplo:
>
> - `route53:CreateHostedZone`
> - `route53domains:RegisterDomain`
> - `route53resolver:CreateResolverEndpoint`

Registro e monitoramento no Amazon Route 53

O Amazon Route 53 fornece log de consultas de DNS e a capacidade de monitorar seus recursos usando as verificações de integridade. Além disso, o Route 53 se integra a outros produtos da AWS para fornecer monitoramento e registro adicionais:

Registrar consultas ao DNS em log

Você pode configurar o Route 53 para registrar informações sobre as consultas que o Route 53 recebe, como o domínio ou o subdomínio que foi solicitado, a data e hora da solicitação e o tipo de registro de DNS, como A ou AAAA.

Para obter mais informações, consulte Log de consultas de DNS pública.

Usar o AWS CloudTrail para registrar em log ações programáticas e do console

O CloudTrail fornece um registro de ações do Route 53 executadas por um usuário, uma função ou um produto da AWS. Usando as informações coletadas pelo CloudTrail, é possível rastrear as solicitações feitas, os endereços IP dos quais a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais. Para obter mais informações, consulte Registro de chamadas de API do Amazon Route 53 com AWS CloudTrail.

Monitorar registros de domínio

O painel do Route 53 fornece informações detalhadas sobre o status dos seus registros de domínio, como o status das transferências de domínio, e domínios que estão se aproximando da data de validade.

Para obter mais informações, consulte Monitorar registros de domínio.

Usar verificações de integridade do Route 53 e o Amazon CloudWatch para monitorar seus recursos

Você pode monitorar seus recursos criando verificações de integridade do Route 53 que utilizam o CloudWatch para coletar e processar dados brutos em métricas legíveis e em tempo quase real.

Para obter mais informações, consulte Monitorando seus recursos com as verificações de saúde do Amazon Route 53 e a Amazon CloudWatch.

Usar o Amazon CloudWatch para monitorar endpoints do Route 53 Resolver

Você pode usar o CloudWatch para monitorar o número de consultas de DNS que são encaminhadas por endpoints do Resolver.

Para obter mais informações, consulte Monitorando endpoints do Route 53 Resolver com a Amazon CloudWatch.

Usar o AWS Trusted Advisor

O Trusted Advisor faz uso das práticas recomendadas aprendidas com o atendimento a clientes da AWS. O Trusted Advisor inspeciona seu ambiente da AWS e faz recomendações quando há oportunidades para economizar dinheiro, melhorar a performance e a disponibilidade do sistema, ou ajuda a corrigir falhas de segurança. Todos os clientes da AWS têm acesso a cinco verificações do Trusted Advisor. Os clientes com um plano de suporte Business ou Enterprise podem ver todas as verificações do Trusted Advisor.

Para obter mais informações, consulte Trusted Advisor.

Validação de conformidade do Amazon Route 53

Auditores externos avaliam a segurança e a conformidade do Amazon Route 53 como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos produtos da AWS no escopo de programas de conformidade específicos, consulte Produtos da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Route 53 é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. Se o seu uso do Route 53 estiver sujeito à conformidade com padrões como HIPAA, PCI ou FedRAMP, a AWS fornecerá recursos para ajudar:

- Guias de início rápido de segurança e conformidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para a implantação de ambientes de linha de base concentrados em conformidade e segurança na AWS.
- Whitepaper Architecting for HIPAA Security and Compliance: este whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- Recursos de conformidade da AWS: esta coleção de manuais e guias pode se aplicar a seu setor e local.
- AWS Config: esse serviço da AWS avalia até que ponto suas configurações de recursos atendem adequadamente às práticas internas e às diretrizes e regulamentações do setor.
- AWS Security Hub: esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

Resiliência no Amazon Route 53

A infraestrutura global da AWS é criada com base em regiões da AWS e zonas de disponibilidade. As regiões da AWS As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, as quais são conectadas com baixa latência, alto throughput e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção.

As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

O Route 53 divide sua funcionalidade em um ambiente de gerenciamento e um plano de dados. O serviço Route 53, como a maioria dos serviços da AWS, inclui um ambiente de gerenciamento que permite executar operações de gerenciamento, como criar, atualizar e excluir recursos, e um plano de dados que fornece a funcionalidade principal do serviço. Para obter mais informações sobre como configurar o DNSSEC no Route 53, consulte Conceitos de planos de dados e de controle.

O Route 53 é basicamente um serviço global, mas os seguintes recursos oferecem suporte às regiões da AWS:

- Se estiver usando o Route 53 Resolver para definir as configurações híbridas, você criará endpoints em regiões da AWS que escolher e especificará endereços IP em várias zonas de disponibilidade. Para endpoints de saída, você cria regras na mesma região onde criou o endpoint. Para obter mais informações, consulte O que Amazon Route 53 Resolveré.
- Você pode configurar verificações de integridade do Route 53 para verificar a integridade dos recursos que você cria em regiões específicas, como instâncias do Amazon EC2 e balanceadores de carga do Elastic Load Balancing.
- Quando você cria uma verificação de integridade que monitora um endpoint, você pode opcionalmente especificar as regiões nas quais deseja que o Route 53 execute verificações de integridade.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Segurança da infraestrutura no Amazon Route 53

Como um serviço gerenciado, o Amazon Route 53 é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Route 53 por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Como monitorar o Amazon Route 53

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho de suas AWS soluções. Você deve coletar dados de monitoramento de todas as partes da sua AWS solução para poder depurar com mais facilidade uma falha de vários pontos, caso ocorra. No entanto, antes de iniciar o monitoramento, é necessário criar um plano que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Tópicos

Log de consultas de DNS pública

É possível configurar o Amazon Route 53 para registrar informações sobre as consultas públicas de DNS recebidas pelo Route 53, como as seguintes:

- O domínio ou o subdomínio que foi solicitado

- Data e hora da solicitação
- Tipo de registro DNS (como A ou AAAA)
- O ponto de presença do Route 53 que respondeu à consulta DNS
- O código de resposta DNS, como `NoError` ou `ServFail`

Depois de configurar o registro de consultas, o Route 53 enviará registros para o CloudWatch Logs. Você usa CloudWatch as ferramentas de registros para acessar os registros de consulta.

Os logs de consulta contêm apenas as consultas que os resolvedores DNS encaminham para o Route 53. Se o resolvedor de DNS já tiver armazenado em cache a resposta a uma consulta (como o endereço IP de um balanceador de carga para example.com), o resolvedor continuará a retornar a resposta armazenada em cache sem encaminhar a consulta para o Route 53 até que o TTL do registro correspondente expire.

Dependendo da quantidade de consultas DNS enviadas a um nome de domínio (example.com) ou nome de subdomínio (www.example.com), de quais resolvedores seus usuários estão usando e do TTL do registro, os logs de consulta poderão conter informações apenas sobre uma das milhares de consultas que são enviadas aos resolvedores de DNS. Para mais informações sobre como o DNS funciona, consulte Como o tráfego da Internet é roteado para seu site ou o aplicativo web.

Se você não precisar de informações detalhadas de registro, poderá usar as CloudWatch métricas da Amazon para ver o número total de consultas de DNS às quais o Route 53 responde em uma zona hospedada. Para ter mais informações, consulte Visualizar métricas de consulta de DNS para uma zona hospedada pública.

Tópicos

Configurar o registro em log para consultas DNS

Para iniciar o registro em log de consultas de DNS para uma zona hospedada especificada, você executa as seguintes tarefas no console do Amazon Route 53:

- Escolha o grupo de CloudWatch registros no qual você deseja que o Route 53 publique registros ou crie um novo grupo de registros.

  > **Note**
  >
  > O grupo de logs deve estar na região Leste dos EUA (Norte da Virgínia).

- Selecione Create (Criar) para terminar.

> **Note**
>
> Se os usuários estiverem enviando consultas de DNS para seu domínio, você deverá começar a ver consultas nos logs vários minutos após criar a configuração de registro de consultas.

Para configurar o registro em log para consultas DNS

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha a zona hospedada para a qual você quer configurar o log de consultas.
4. No painel Hosted zone details, escolha Configure query logging.
5. Escolha um grupo de logs existente ou crie um novo grupo de logs.
6. Se você receber um alerta sobre permissões (isso acontece se você não tiver configurado o log de consultas com o novo console antes), siga um destes procedimentos:

   - Se já tiver dez políticas de recursos, você não poderá criar mais. Selecione qualquer uma das políticas de recursos e selecione Edit (Editar). A edição dará ao Route 53 permissões para gravar logs em seus grupos de logs. Selecione Save (Salvar). O alerta desaparece e você pode continuar na próxima etapa.

- Se você nunca configurou o registro de consultas antes (ou se ainda não criou 10 políticas de recursos), você precisa conceder permissões ao Route 53 para gravar registros em seus grupos de CloudWatch registros. Escolha Grant permissions (Conceder permissões). O alerta desaparece e você pode continuar na próxima etapa.

7. Escolha Permissões - opcional para ver uma tabela que mostra se a política de recursos corresponde ao grupo de CloudWatch registros e se o Route 53 tem permissão para publicar registros no CloudWatch.
8. Selecione Create (Criar).

Usando CloudWatch a Amazon para acessar registros de consultas de DNS

O Amazon Route 53 envia registros de consulta diretamente para o CloudWatch Logs; os registros nunca são acessíveis por meio do Route 53. Em vez disso, você usa CloudWatch Logs para visualizar registros quase em tempo real, pesquisar e filtrar dados e exportar registros para o Amazon S3.

O Route 53 cria um fluxo de CloudWatch registros para cada ponto de borda do Route 53 que responde às consultas de DNS para a zona hospedada especificada e envia os registros de consulta para o fluxo de registros aplicável. O formato do nome de cada fluxo de log é *hosted-zone-id*/*edge-location-ID*, por exemplo, `Z1D633PJN98FT9/DFW3`.

Cada ponto de presença é identificado por um código de três letras e um número atribuído arbitrariamente, por exemplo, DFW3. O código de três letras normalmente corresponde ao código da Associação Internacional de Transportes Aéreos de um aeroporto perto do ponto de presença. (Essas abreviações podem mudar no futuro.) Para obter uma lista dos pontos de presença, consulte "A rede global do Route 53" na página Detalhes do produto Route 53.

> **Note**
>
> Talvez você veja alguns prefixos ou sufixos que não seguem a convenção acima. Esses codificam atributos que são somente para uso interno.

Para obter mais informações, consulte a documentação aplicável:

- Guia do usuário do Amazon CloudWatch Logs

- Referência da API Amazon CloudWatch Logs
- CloudWatch Seção Logs da Referência de AWS CLI Comandos
- Valores que aparecem em logs de consultas de DNS

Alterar o período de retenção para logs e exportar logs para o Amazon S3

Por padrão, o CloudWatch Logs armazena registros de consultas indefinidamente. Opcionalmente, você pode especificar um período de retenção para que o CloudWatch Logs exclua os registros mais antigos do que o período de retenção. Para obter mais informações, consulte Alterar a retenção de dados de log em CloudWatch Logs no Guia CloudWatch do usuário da Amazon.

Se você quiser reter dados de log, mas não precisar de ferramentas de CloudWatch registros para visualizar e analisar os dados, você pode exportar registros para o Amazon S3, o que pode reduzir seus custos de armazenamento. Para obter mais informações, consulte Como exportar dados de log para o Amazon S3.

Para obter informações sobre definição de preço, consulte a página de definição de preço aplicável:

- “Amazon CloudWatch Logs” na página CloudWatch de preços
- Preços do Amazon S3

> **Note**
>
> Quando você configura o Route 53 para registrar consultas de DNS, você não recebe cobranças do Route 53.

Interromper o registro de consultas em log

Se você quiser que o Amazon Route 53 pare de enviar registros de consulta para CloudWatch Logs, execute o procedimento a seguir para excluir a configuração de registro de consultas.

Para excluir a configuração do registro em log de consultas

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.

3. Escolha o nome da zona hospedada da qual você quer excluir a configuração de log de consultas.
4. No painel Hosted zone details (Detalhes da zona hospedada), escolha Configure query logging (Configurar log de consultas).
5. Escolha Delete para confirmar.

Valores que aparecem em logs de consultas de DNS

Cada arquivo de log contém uma entrada de log para cada consulta de DNS recebida pelo Amazon Route 53 de resolvedores de DNS no local da borda correspondente. Cada entrada do log inclui os seguintes valores:

Versão do formato do log

O número da versão deste log de consulta. Se você adicionar campos ao log ou alterar o formato dos campos existentes, incrementaremos esse valor.

Timestamp da consulta

A data e a hora na qual o Route 53 respondeu à solicitação, no formato ISO 8601 e no Tempo Universal Coordenado (UTC), por exemplo, `2017-03-16T19:20:25.177Z`.

Para obter informações sobre o formato ISO 8601, consulte o artigo ISO 8601 na Wikipédia. Para obter informações sobre UTC, consulte o artigo Tempo Universal Coordenado na Wikipédia.

ID da hosted zone

O ID da zona hospedada associada a todas as consultas DNS neste log.

Nome da consulta

O domínio ou o subdomínio que foi especificado na solicitação.

Tipo da consulta

O tipo de registro DNS que foi especificado na solicitação ou `ANY`. Para obter informações sobre os tipos com suporte do Route 53, consulte Tipos de registro de DNS com suporte.

Código de resposta

O código de resposta do DNS que o Route 53 retornou em resposta à consulta de DNS.

Protocolo da camada 4

O protocolo que foi usado para enviar a consulta, `TCP` ou `UDP`.

Local do borda do Route 53

O local da borda do Route 53 que respondeu à consulta. Cada ponto de presença é identificado por um código de três letras e um número arbitrário, por exemplo, DFW3. O código de três letras normalmente corresponde ao código da Associação Internacional de Transportes Aéreos de um aeroporto perto do ponto de presença. (Essas abreviações podem mudar no futuro.)

Para obter uma lista dos locais da borda, consulte “A rede global do Route 53” na página Route 53 Product Detail (Detalhes do produto Route 53).

Endereço IP do resolvedor

O endereço IP do resolvedor de DNS que enviou a solicitação ao Route 53.

Sub-rede do cliente EDNS

Um endereço IP parcial do cliente do qual a solicitação se originou, se disponível no resolvedor de DNS.

Para obter mais informações, consulte o rascunho do IETF Sub-rede de cliente em solicitações DNS.

Exemplo de log de consulta

Aqui está um exemplo de log de consulta (A região é um espaço reservado):

```
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 -
```

Log de consultas do Resolver

Você pode registrar as seguintes consultas de DNS:

- Consultas originadas nas VPCs do Amazon Virtual Private Cloud especificadas por você, bem como as respostas a essas consultas de DNS.
- Consultas de recursos on-premises que usam um endpoint do Resolver de entrada.
- Consultas que usam um endpoint do Resolver de saída para resolução de DNS recursiva.
- Consultas que usam regras do Firewall DNS do Route 53 Resolver para bloquear, permitir ou monitorar listas de domínios.

Os logs de consulta do Resolver incluem valores como os seguintes:

- A AWS região em que o VPC foi criado
- O ID da VPC da qual a consulta se originou
- O endereço IP da instância da qual a consulta se originou
- O ID da instância do recurso do qual a consulta se originou
- Data e hora em que a consulta foi feita pela primeira vez
- O nome DNS solicitado (como, prod.example.com)
- O tipo de registro DNS (como A ou AAAA)
- O código de resposta DNS, como, por exemplo, `NoError` ou `ServFail`
- Os dados de resposta do DNS, como o endereço IP que é retornado em resposta à consulta de DNS
- Uma resposta a uma ação de regra do Firewall DNS

Para obter uma lista detalhada de todos os valores registrados e um exemplo, consulte Valores que aparecem em logs de consultas do Resolver.

> **Note**
>
> Como é padrão para resolvedores de DNS, os resolvedores armazenam em cache as consultas de DNS por um período determinado pelo time-to-live (TTL) do resolvedor. O Route 53 Resolver armazena em cache consultas originadas em suas VPCs e responde do cache sempre que possível para acelerar as respostas. O log de consultas do Resolver registra apenas consultas exclusivas, não consultas às quais o Resolver pode responder usando o cache.
>
> Por exemplo, suponha que uma instância do EC2 em uma das VPCs, para as quais uma configuração de log de consultas está registrando consultas, envie uma solicitação para

accounting.example.com. O Resolver armazena em cache a resposta a essa consulta e registra a consulta. Se a interface de rede elástica da mesma instância fizer uma consulta para accounting.example.com dentro do TTL do cache do Resolver, o Resolver responderá à consulta do cache. A segunda consulta não é registrada.

Você pode enviar os registros para um dos seguintes AWS recursos:

- Grupo de CloudWatch registros Amazon CloudWatch Logs (Logs)
- Bucket do Amazon S3 (S3)
- Fluxo de entrega do Firehose

Para ter mais informações, consulte AWS recursos para os quais você pode enviar registros de consulta do Resolver.

Tópicos

AWS recursos para os quais você pode enviar registros de consulta do Resolver

> **Note**
>
> Se você pretende registrar consultas para workloads com altas consultas por segundo (QPS), use o Amazon S3 para garantir que seus logs de consultas não sejam limitados quando gravados em seu destino. Se você usa a Amazon CloudWatch, pode aumentar o limite de solicitações por segundo para a `PutLogEvents` operação. Para saber mais sobre como aumentar seus CloudWatch limites, consulte CloudWatch Registrar cotas no Guia do CloudWatch usuário da Amazon.

Você pode enviar registros de consulta do Resolver para os seguintes AWS recursos:

Grupo de CloudWatch registros Amazon CloudWatch Logs (Amazon Logs)

Você pode analisar logs com o Logs Insights e criar métricas e alarmes.

Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

Bucket do Amazon S3 (S3)

Um bucket do S3 é econômico para arquivamento de logs em longo prazo. A latência geralmente é maior.

Todas as opções de criptografia do lado do servidor do S3 são compatíveis. Para obter mais informações, consulte Proteger os dados usando criptografia do lado do servidor no Guia do usuário do Amazon S3.

Se o bucket do S3 estiver em uma conta que você possui, as permissões necessárias serão adicionadas automaticamente à sua política de bucket. Se você quiser enviar logs para um bucket do S3 em uma conta que você não possui, o proprietário do bucket do S3 deverá adicionar permissões para sua conta em sua política de bucket. Por exemplo:

```
{
    "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 você quiser armazenar logs em um bucket do S3 central para sua organização, recomendamos que você configure sua configuração de log de consultas a partir de uma conta centralizada (com as permissões necessárias para gravar em um bucket central) e use a RAM para compartilhar a configuração entre contas.

Para obter mais detalhes, consulte o Manual do usuário do Amazon Simple Storage Service.

Fluxo de entrega do Firehose

Você pode transmitir logs em tempo real para o Amazon OpenSearch Service, o Amazon Redshift ou outros aplicativos.

Para obter mais informações, consulte o Guia do desenvolvedor do Amazon Data Firehose.

Para obter informações sobre os preços do registro de consultas do Resolver, consulte os CloudWatch preços da Amazon.

CloudWatch As cobranças de registros se aplicam ao usar os registros do Resolver, mesmo quando os registros são publicados diretamente no Amazon S3. Para obter mais informações, consulte Entregar registros para o S3 de acordo com os CloudWatch preços da Amazon.

Como gerenciar configurações de log de consultas do Resolver

Como configurar (log de consultas do Resolver)

Para iniciar o registro de consultas de DNS que se originam em suas VPCs, você executa as seguintes tarefas no console do Amazon Route 53:

Para configurar o log de consultas do Resolver

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Expanda o menu do console do Route 53. No canto superior esquerdo do console, escolha o ícone de três barras horizontais (☰).
3. No menu Resolver, escolha Query logging (Log de consultas).
4. No seletor de região, escolha a AWS região em que você deseja criar a configuração de registro de consultas. Essa deve ser a mesma região onde você criou as VPCs para as quais quer registrar consultas ao DNS em log. Se você tiver VPCs em várias regiões, deverá criar pelo menos uma configuração do log de consultas para cada região.
5. Escolha Configure query logging (Configurar log de consultas).
6. Especifique os seguintes valores:

   Nome da configuração do log de consultas

   Insira um nome para sua configuração do log de consultas. O nome é exibido no console na lista de configurações do log de consultas. Insira um nome que o ajudará a encontrar essa configuração posteriormente.

   Destino dos logs de consulta

   Escolha o tipo de AWS recurso para o qual você deseja que o Resolver envie registros de consulta. Para obter informações sobre como escolher entre as opções (grupo de CloudWatch registros de registros, bucket do S3 e stream de entrega do Firehose), consulte. AWS recursos para os quais você pode enviar registros de consulta do Resolver

   Depois de escolher o tipo de recurso, você pode criar outro recurso desse tipo ou escolher um recurso existente criado pela AWS conta atual.

   > **Note**
   >
   > Você pode escolher somente os recursos que foram criados na AWS região que você escolheu na etapa 4, a região em que você está criando a configuração de registro de consultas. Se você optar por criar um novo recurso, esse recurso será criado na mesma região.

VPCs para as quais registrar consultas em log

Essa configuração de log de consultas registrará consultas de DNS originadas nas VPCs que você escolher. Marque a caixa de seleção de cada VPC na região atual para a qual deseja que o Resolver registre consultas e escolha Choose (Escolher).

> **Note**
>
> A entrega de log da VPC pode ser habilitada apenas uma vez para um tipo de destino específico. Os logs não podem ser entregues a vários destinos do mesmo tipo, por exemplo, os logs da VPC não podem ser entregues a dois destinos do Amazon S3.

7. Escolha Configure query logging (Configurar log de consultas).

> **Note**
>
> Você deve começar a ver consultas de DNS feitas por recursos em sua VPC nos logs em alguns minutos após a criação bem-sucedida da configuração do log de consultas.

Valores que aparecem em logs de consultas do Resolver

Cada arquivo de log contém uma entrada de log para cada consulta de DNS recebida pelo Amazon Route 53 de resolvedores de DNS no local da borda correspondente. Cada entrada do log inclui os seguintes valores:

versão

O número da versão do formato do log de consulta. A versão atual é `1.1`.

O valor da chave é uma versão principal e secundária no formulário **`major_version.minor_version`**. Por exemplo, você pode ter um valor de `version` de `1.7`, onde 1 é a versão principal, e 7 é a versão secundária.

O Route 53 incrementa a versão principal, se uma alteração for feita para a estrutura do log que não é compatível com as versões anteriores. Isso inclui a remoção de um campo JSON que

já está presente ou a alteração de como os conteúdos de um campo são representados (por exemplo, um formato de data).

O Route 53 incrementa a versão secundária se uma alteração adicionar novos campos ao arquivo de log. Isso pode ocorrer se novas informações estiverem disponíveis para algumas ou todas as consultas DNS existentes em uma VPC.

account_id

O ID da AWS conta que criou a VPC.

região

A AWS região na qual você criou a VPC.

vpc_id

O ID da VPC na qual a consulta se originou.

query_timestamp

A data e a hora em que a consulta foi submetida, no formato ISO 8601 e no Tempo Universal Coordenado (UTC), por exemplo, `2017-03-16T19:20:177Z`.

Para obter informações sobre o formato ISO 8601, consulte o artigo ISO 8601 na Wikipédia. Para obter informações sobre UTC, consulte o artigo Tempo Universal Coordenado na Wikipédia.

query_name

O nome de domínio (example.com) ou de subdomínio (www.example.com) especificado na consulta.

query_type

O tipo de registro DNS que foi especificado na solicitação ou `ANY`. Para obter informações sobre os tipos com suporte do Route 53, consulte Tipos de registro de DNS com suporte.

query_class

A classe da consulta.

rcode

O código de resposta do DNS que o Resolver retornou em resposta à consulta de DNS. Um código de resposta que indica se a consulta foi válida ou não. O código de resposta mais comum é `NOERROR` e indica que a consulta foi válida. Se a resposta não for válida, o Resolver retornará

um código de resposta que explica o motivo. Para obter uma lista dos códigos de resposta possíveis, consulte DNS RCODES no site da IANA.

responder_type

O tipo de registro DNS (como A, MX ou CNAME) do valor que o Resolver está retornando em resposta à consulta. Para obter informações sobre os tipos com suporte do Route 53, consulte Tipos de registro de DNS com suporte.

rdata

O valor que o Resolver retornou em resposta à consulta. Por exemplo, para um registro A, este é um endereço IP no formato IPv4. Para um registro CNAME, este é o nome de domínio no registro CNAME.

answer_class

A classe da resposta do Resolver para a consulta.

srcaddr

O endereço IP da instância na qual a consulta se originou.

srcport

A porta na instância na qual a consulta se originou.

transport

O protocolo usado para enviar a consulta de DNS.

srcids

Os IDs de `instance`, `resolver_endpoint` e `resolver_network_interface` dos quais a consulta de DNS se originou ou pelos quais passou.

instância

O ID da instância da qual a consulta se originou.

resolver_endpoint

O ID do endpoint do resolvedor que passa a consulta de DNS para servidores DNS on-premises.

firewall_rule_group_id

O ID do grupo de regras do Firewall DNS que correspondeu ao nome de domínio na consulta. Esta opção é preenchida somente se o Firewall DNS encontrar uma correspondência para uma regra com a ação definida como alerta ou bloqueio.

Para obter mais informações sobre grupos de regras de firewall, consulte Regras e grupos de regras do Firewall DNS.

firewall_rule_action

A ação especificada pela regra que correspondeu ao nome de domínio na consulta. Esta opção é preenchida somente se o Firewall DNS encontrar uma correspondência para uma regra com a ação definida como alerta ou bloqueio.

firewall_domain_list_id

A lista de domínios usada pela regra que correspondeu ao nome de domínio na consulta. Esta opção é preenchida somente se o Firewall DNS encontrar uma correspondência para uma regra com a ação definida como alerta ou bloqueio.

propriedades_adicionais

Informações adicionais sobre os eventos de entrega de log. is_delayed: se houver um atraso na entrega dos logs.

Exemplo de log de consultas do Route 53 Resolver

Aqui está um exemplo de log de consultas do 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"
    }
```

Compartilhando configurações de registro de consultas do Resolver com outras contas AWS

Você pode compartilhar as configurações de registro de consultas que você criou usando uma AWS conta com outras AWS contas. Para compartilhar configurações, o console do Route 53 Resolver se integra ao AWS Resource Access Manager. Para obter mais informações sobre o Resource Access Manager, consulte o Guia do usuário do Resource Access Manager.

Observe o seguinte:

Como associar VPCs a configurações de log de consultas compartilhadas

Se outra AWS conta tiver compartilhado uma ou mais configurações com sua conta, você poderá associar VPCs à configuração da mesma forma que associa VPCs às configurações que você criou.

Como excluir ou cancelar o compartilhamento de uma configuração

Se você compartilhar uma configuração com outras contas e, em seguida, excluir a configuração ou parar de compartilhá-la, e se uma ou mais VPCs foram associadas à configuração, o Route 53 Resolver irá parar de registrar consultas de DNS com origem nessas VPCs.

Número máximo de configurações de log de consultas e VPCs que podem ser associadas a uma configuração

Quando uma conta cria uma configuração e a compartilha com uma ou mais contas, o número máximo de VPCs que podem ser associadas à configuração se aplicam por conta. Por exemplo, se você tiver 10.000 contas em sua organização, poderá criar a configuração de registro de consultas na conta central e compartilhá-la por meio de AWS RAM para compartilhá-la com as contas da organização. Em seguida, as contas da organização associarão a configuração às VPCs, contando-as com base nas associações de VPC da configuração do log de consultas da conta por Região da AWS limite de 100. No entanto, se todas as VPCs estiverem em uma única conta, talvez seja necessário aumentar os limites de serviço da conta.

Para as cotas atuais do Resolver, consulte Cotas no Route 53 Resolver.

Permissões

Para compartilhar uma regra com outra AWS conta, você precisa ter permissão para usar a PutResolverQueryLogConfigPolicyação.

Restrições na AWS conta com a qual uma regra é compartilhada

A conta com a qual uma regra é compartilhada não pode alterar ou excluir a regra.

Tags

Somente a conta que criou uma regra pode adicionar, excluir ou consultar tags na regra.

Para visualizar o status de compartilhamento atual de uma regra (incluindo a conta que compartilhou a regra ou a conta com a qual uma regra é compartilhada) e para compartilhar regras com outra conta, realize o procedimento a seguir.

Para exibir o status de compartilhamento e compartilhar configurações de log de consultas com outra conta da AWS

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Query Logging (Log de consultas).
3. Na barra de navegação, escolha a Região onde a regra foi criada.

   A coluna Sharing status (Status de compartilhamento) mostra o status de compartilhamento atual das regras criadas pela conta atual ou que foram compartilhadas com a conta atual:

   - Não compartilhada: a AWS conta atual criou a regra e a regra não é compartilhada com nenhuma outra conta.
   - Shared by me (Compartilhada por mim): a conta atual criou a regra e compartilhou com uma ou mais contas.
   - Shared with me (Compartilhada comigo): outra conta criou a regra e compartilhou com a conta atual.
4. Escolha o nome da regra para a qual deseja exibir informações de compartilhamento ou que deseja compartilhar com outra conta.

   Na página Rule: ***rule name*** (Regra: nome da regra), o valor em Owner (Proprietário) exibe o ID da conta da que criou a regra. Essa é a conta atual, a menos que o valor do Sharing status

(Status de compartilhamento) seja Shared with me (Compartilhada comigo). Neste caso, Owner (Proprietário) é a conta que criou a regra e compartilhou com a conta atual.

5. Escolha Share (Compartilhar) para visualizar informações adicionais ou para compartilhar a regra com outra conta. Uma página no console do Resource Access Manager é exibida, dependendo do valor de Sharing status (Status de compartilhamento):

   - Não compartilhada: a página Create resource share (Criar compartilhamento de recurso) é exibida. Para obter informações sobre como compartilhar a regra com outra conta, OU ou organização, pule para a etapa 6.
   - Compartilhada por mim: a página Shared resources (Recursos compartilhados) mostra as regras e outros recursos de propriedade da conta atual e compartilhados com outras contas.
   - Compartilhada comigo: a página Shared resources (Recursos compartilhados) mostra as regras e outros recursos de propriedade de outras contas e compartilhados com a conta atual.

6. Para compartilhar uma configuração de registro de consultas com outra AWS conta, OU ou organização, especifique os valores a seguir.

   > **Note**
   >
   > Não é possível atualizar as configurações de compartilhamento. Se quiser alterar qualquer uma das configurações a seguir, é necessário compartilhar a regra novamente com as novas configurações e, em seguida, remover as configurações de compartilhamento antigas.

   Descrição

   Insira uma breve descrição que ajude a lembrar o motivo do compartilhamento da configuração de registro de consulta.

   Recursos

   Marque a caixa de seleção da configuração que você quer compartilhar.

   Entidades principais

   Insira o número da AWS conta, nome da OU ou nome da organização.

Tags

Especifique uma ou mais chaves e os valores correspondentes. Por exemplo, você pode especificar o Cost center (Centro de custo) para Key (Chave) e especificar 456 para Value (Valor).

Essas são as tags que AWS Billing and Cost Management permitem organizar sua AWS fatura; você também pode usar tags para outros fins. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing .

Monitorar registros de domínio

O painel do Amazon Route 53 fornece informações detalhadas sobre o status dos seus registros de domínio, incluindo:

- Status dos novos registros de domínio
- Status das transferências de domínio para o Route 53
- Lista dos domínios cujas datas de expiração estão próximas

Recomendamos verificar periodicamente o painel no console do Route 53, principalmente depois de registrar um novo domínio ou transferir um domínio para o Route 53, para confirmar se não há problemas a serem corrigidos.

Recomendamos também que você verifique se as informações de contato dos seus domínios estão atualizadas. Quando a data de expiração de um domínio estiver próxima, enviaremos um e-mail ao contato registrante do domínio contendo informações sobre quando o domínio expirará e como renová-lo.

Monitorando seus recursos com as verificações de saúde do Amazon Route 53 e a Amazon CloudWatch

Você pode monitorar seus recursos criando verificações de saúde do Amazon Route 53, que são usadas CloudWatch para coletar e processar dados brutos em métricas legíveis e quase em tempo real. Essas estatísticas são registradas por um período de duas semanas, de maneira que você possa acessar informações do histórico e ter uma perspectiva melhor sobre o desempenho dos

seus recursos. Por padrão, os dados métricos das verificações de saúde do Route 53 são enviados automaticamente CloudWatch em intervalos de um minuto.

Para obter mais informações sobre as verificações de integridade do Route 53 consulte Como monitorar as verificações de integridade usando o CloudWatch. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

Métricas e dimensões para verificações de integridade do Route 53

Quando você cria uma verificação de saúde, o Amazon Route 53 começa a enviar métricas e dimensões uma vez por minuto para CloudWatch aproximadamente o recurso que você especifica. No console do Route 53, é possível visualizar o status das suas verificações de integridade. Você também pode usar os procedimentos a seguir para visualizar as métricas no CloudWatch console ou visualizá-las usando o AWS Command Line Interface (AWS CLI).

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Na guia Todas as métricas, escolha Route 53.
4. Escolha Métricas de verificação de integridade.

Para visualizar métricas usando o AWS CLI

- Em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

Tópicos

- CloudWatch métricas para verificações de saúde do Route 53
- Dimensões para métricas de verificações de integridade do Route 53

CloudWatch métricas para verificações de saúde do Route 53

O namespace `AWS/Route53` inclui as métricas a seguir para verificações de integridade do Route 53.

ChildHealthCheckHealthyContagem

Para uma verificação de estado de integridade, o número de verificações de integridade íntegras.

Estatísticas válidas: média (recomendada), mínimo, máximo

Unidades: contagem

ConnectionTime

O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para estabelecer uma conexão TCP com o endpoint. Você pode visualizar `ConnectionTime` para uma verificação de saúde em todas as regiões ou para uma região selecionada.

Estatísticas válidas: média (recomendada), mínimo, máximo

Unidade: milissegundos

HealthCheckPercentageHealthy

O percentual dos verificadores de integridade do Route 53 que consideram o endpoint selecionado íntegro.

Estatísticas válidas: média, mínimo, máximo

Unidades: percentual

HealthCheckStatus

O status do endpoint de verificação de saúde que CloudWatch está sendo verificado. 1 indica saudável e 0 indica insalubre.

Estatísticas válidas: mínimo, máximo e média

Unidades: nenhuma

SSL HandshakeTime

O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para concluir o handshake do SSL. Você pode visualizar `SSLHandshakeTime` para uma verificação de saúde em todas as regiões ou para uma região selecionada.

Estatísticas válidas: média (recomendada), mínimo, máximo

Unidade: milissegundos

TimeToFirstByte

O tempo médio, em milissegundos, que os verificadores de integridade do Route 53 levaram para receber o primeiro byte da resposta a uma solicitação HTTP ou HTTPS. Você pode visualizar `TimeToFirstByte` para uma verificação de saúde em todas as regiões ou para uma região selecionada.

Estatísticas válidas: média (recomendada), mínimo, máximo

Unidade: milissegundos

Dimensões para métricas de verificações de integridade do Route 53

As métricas do Route 53 para verificações de integridade usam o namespace do `AWS/Route53` e fornecem métricas para `HealthCheckId`. Ao recuperar métricas, você deve fornecer a dimensão `HealthCheckId`.

Além disso, para `ConnectionTime`, `SSLHandshakeTime` e `TimeToFirstByte`, você pode opcionalmente especificar `Region`. Se você omitir`Region`, CloudWatch retornará métricas em todas as regiões. Se você incluir`Region`, CloudWatch retornará métricas somente para a região especificada.

Para ter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

Monitoramento de zonas hospedadas usando a Amazon CloudWatch

Você pode monitorar suas zonas públicas hospedadas usando CloudWatch a Amazon para coletar e processar dados brutos em métricas legíveis e quase em tempo real. As métricas estão disponíveis logo após o Route 53 receber as consultas de DNS nas quais as métricas se baseiam. CloudWatch os dados métricos das zonas hospedadas do Route 53 têm uma granularidade de um minuto.

Para obter mais informações, consulte a documentação a seguir

- Para obter uma visão geral e informações sobre como visualizar métricas no CloudWatch console da Amazon e como recuperar métricas usando o AWS Command Line Interface (AWS CLI), consulte Visualizar métricas de consulta de DNS para uma zona hospedada pública

- Para obter informações sobre o período de retenção das métricas, consulte GetMetricEstatísticas na Amazon CloudWatch API Reference.
- Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.
- Para obter mais informações sobre CloudWatch métricas, consulte Usando CloudWatch métricas da Amazon no Guia CloudWatch do usuário da Amazon.

Tópicos

CloudWatch métricas para zonas hospedadas públicas do Route 53

O namespace `AWS/Route53` inclui as seguintes métricas para zonas hospedadas do Route 53:

DNSQueries

Para uma zona hospedada, o número de consultas de DNS respondidas pelo Route 53 em um período especificado.

Estatísticas válidas: soma, SampleCount

Unidades: contagem

Região: o Route 53 é um serviço global. Para obter métricas de zonas hospedadas, você deve especificar US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)) para a região.

DNSSEC InternalFailure

O valor será um se qualquer objeto na zona hospedada estiver em um estado INTERNAL_FAILURE. Caso contrário, o valor será zero.

Estatística válida: soma

Unidades: contagem

Volume: 1 por 4 horas por zona hospedada

Região: o Route 53 é um serviço global. Para obter métricas de zonas hospedadas, você deve especificar US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)) para a região.

Ação do DNSSEC KeySigning KeysNeeding

Número de chaves de assinatura (KSKs) que têm um estado ACTION_NEEDED (devido a falha do KMS).

Estatísticas válidas: soma, SampleCount

Unidades: contagem

Volume: 1 por 4 horas por zona hospedada

Região: o Route 53 é um serviço global. Para obter métricas de zonas hospedadas, você deve especificar US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)) para a região.

Era do DNSSEC KeySigning KeyMax NeedingAction

Tempo decorrido desde que a chave de assinatura de chaves (KSK) foi definida para o estado ACTION_NEEDED.

Estatísticas válidas: máximo

Unidades: segundos

Volume: 1 por 4 horas por zona hospedada

Região: o Route 53 é um serviço global. Para obter métricas de zonas hospedadas, você deve especificar US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)) para a região.

DNSSEC KeySigning KeyAge

O tempo decorrido desde que a chave de assinatura de chaved (KSK) foi criada (não desde que foi ativada).

Estatísticas válidas: máximo

Unidades: segundos

Volume: 1 por 4 horas por zona hospedada

Região: o Route 53 é um serviço global. Para obter métricas de zonas hospedadas, você deve especificar US East (N. Virginia) (Leste dos EUA (Norte da Virgínia)) para a região.

CloudWatch dimensão para métricas de zona hospedada pública do Route 53

As métricas do Route 53 para zonas hospedadas usam o namespace `AWS/Route53` e fornecem métricas para `HostedZoneId`. Para obter o número de consultas de DNS, você deve especificar o ID da zona hospedada na dimensão `HostedZoneId`.

Monitorando endpoints do Route 53 Resolver com a Amazon CloudWatch

Você pode usar CloudWatch a Amazon para monitorar o número de consultas de DNS que são encaminhadas pelos endpoints do Route 53 Resolver. A Amazon CloudWatch coleta e processa dados brutos em métricas legíveis, quase em tempo real. Essas estatísticas são registradas por um período de duas semanas, de maneira que você possa acessar informações do histórico e ter uma perspectiva melhor sobre o desempenho dos seus recursos. Por padrão, os dados métricos dos endpoints do Resolver são enviados automaticamente CloudWatch em intervalos de cinco minutos. O intervalo de cinco minutos também é o menor intervalo no qual os dados métricos podem ser enviados.

Para obter mais informações sobre o Resolver, consulte O que Amazon Route 53 Resolveré. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

Métricas e dimensões do Route 53 Resolver

Quando você configura o Resolver para encaminhar consultas de DNS para sua rede ou vice-versa, o Resolver começa a enviar métricas e dimensões uma vez a cada cinco minutos para CloudWatch aproximadamente o número de consultas que são encaminhadas. Você pode usar os procedimentos a seguir para visualizar as métricas no CloudWatch console ou visualizá-las usando o AWS Command Line Interface (AWS CLI).

Para visualizar as métricas do Resolver usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Na barra de navegação, selecione a Região onde você criou o endpoint.
3. No painel de navegação, selecione Métricas.
4. Na guia All metrics (Todas as métricas), selecione Route 53 Resolver (Resolvedor do Route 53).

5. Selecione By Endpoint (Por endpoint) para visualizar as contagens de consultas para um endpoint especificado. Em seguida, selecione os endpoints para os quais você deseja visualizar o número de consultas.

   Escolha Across All Endpoints para visualizar as contagens de consultas para todos os endpoints de entrada ou para todos os endpoints de saída que foram criados pela conta atual. AWS Em seguida, escolha InboundQueryVolume ou OutboundQueryVolume para ver as contagens desejadas.

Para visualizar métricas usando o AWS CLI

- Em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Tópicos

CloudWatch métricas para o Route 53 Resolver

O namespace `AWS/Route53Resolver` inclui métricas para endpoints e endereços IP do Route 53 Resolver.

Tópicos

Métricas para endpoints do Resolver

O namespace `AWS/Route53Resolver` inclui as métricas a seguir para endpoints do Route 53 Resolver.

EndpointHealthyContagem ENIC

O número de interfaces de rede elástica no status `OPERATIONAL`. Isso significa que as interfaces de rede Amazon VPC para o endpoint (especificado pela `EndpointId`) estão configuradas

corretamente e podem passar consultas de DNS de entrada ou saída entre sua rede e o Resolver.

Estatísticas válidas: mínimo, máximo, média

Unidades: contagem

EndpointUnhealthyContagem ENIC

O número de interfaces de rede elástica no status `AUTO_RECOVERING`.

Isso significa que o resolvedor está tentando recuperar uma ou mais interfaces de rede da Amazon VPC associadas ao endpoint (especificado pelo `EndpointId`). Durante o processo de recuperação, o endpoint funciona com capacidade limitada e não consegue processar consultas de DNS até que seja totalmente recuperado.

Estatísticas válidas: mínimo, máximo, média

Unidades: contagem

InboundQueryVolume

Para endpoints de entrada, o número de consultas de DNS encaminhadas da rede para as VPCs por meio do endpoint especificado por `EndpointId`.

Estatística válida: soma

Unidades: contagem

OutboundQueryVolume

Para endpoints de saída, o número de consultas de DNS encaminhadas das VPCs para a rede por meio do endpoint especificado por `EndpointId`.

Estatística válida: soma

Unidades: contagem

OutboundQueryAggregateVolume

Para endpoints de saída, o número total de consultas DNS encaminhadas das Amazon VPCs para sua rede, incluindo o seguinte:

- O número de consultas DNS encaminhadas das VPCs para a rede por meio do endpoint especificado por `EndpointId`.

- Quando a conta atual compartilha regras do Resolver com outras contas, consultas de VPCs criadas por outras contas são encaminhadas para a sua rede por meio do endpoint especificado pelo `EndpointId`.

Estatística válida: soma

Unidades: contagem

Métricas para endereços IP do Resolver

O namespace `AWS/Route53Resolver` inclui as métricas a seguir para cada endereço IP associado a um endpoint de entrada ou saída do Resolver. (Ao especificar um endpoint, o Resolver cria uma interface de rede elástica da Amazon VPC.)

InboundQueryVolume

Para cada endereço IP dos endpoints de entrada, o número de consultas DNS encaminhadas da rede para o endereço IP especificado. Cada endereço IP é identificado pelo ID do endereço IP. É possível obter esse valor usando o console do Route 53. Na página do endpoint aplicável, na seção Endereços IP, consulte a coluna IP address ID (ID do endereço IP). Você também pode obter o valor programaticamente usando ListResolver EndpointIp Endereços.

Estatística válida: soma

Unidades: contagem

OutboundQueryAggregateVolume

Para cada endereço IP para seus endpoints de saída, o número total de consultas DNS encaminhadas das Amazon VPCs para sua rede, incluindo o seguinte:

- O número de consultas DNS encaminhadas de suas VPCs para sua rede usando o endereço IP especificado.
- Quando a conta atual compartilha regras do Resolver com outras contas, consultas de VPCs criadas por outras contas são encaminhadas para a sua rede usando o endereço IP especificado.

Cada endereço IP é identificado pelo ID do endereço IP. É possível obter esse valor usando o console do Route 53. Na página do endpoint aplicável, na seção Endereços IP, consulte a coluna IP address ID (ID do endereço IP). Você também pode obter o valor programaticamente usando ListResolver EndpointIp Endereços.

Estatística válida: soma

Unidades: contagem

Dimensões das métricas do Route 53 Resolver

As métricas do Route 53 Resolver para endpoints de entrada e de saída usam o namespace `AWS/Route53Resolver` e fornecem métricas para `EndpointId`. Se você especificar um valor para a `EndpointId` dimensão, CloudWatch retornará o número de consultas de DNS para o endpoint especificado. Se você não especificar`EndpointId`, CloudWatch retornará o número de consultas DNS para todos os endpoints que foram criados pela conta atual. AWS

A dimensão `RniId` é compatível com as métricas `OutboundQueryAggregateVolume` e `InboundQueryVolume`.

Monitorando grupos de regras do firewall DNS do Route 53 Resolver com a Amazon CloudWatch

Você pode usar CloudWatch a Amazon para monitorar o número de consultas de DNS que são filtradas pelos grupos de regras do Route 53 Resolver DNS Firewall. A Amazon CloudWatch coleta e processa dados brutos em métricas legíveis, quase em tempo real. Essas estatísticas são registradas por um período de duas semanas, de maneira que você possa acessar informações do histórico e ter uma perspectiva melhor sobre o desempenho dos seus recursos. Por padrão, os dados métricos dos grupos de regras do Firewall DNS são enviados automaticamente CloudWatch em intervalos de cinco minutos.

Para obter mais informações sobre o Firewall de DNS, consulte Firewall de DNS do Route 53 Resolver. Para obter mais informações sobre CloudWatch, consulte O que é a Amazon CloudWatch? no Guia do CloudWatch usuário da Amazon.

Métricas e dimensões do Firewall DNS do Route 53 Resolver

Quando você associa um grupo de regras do Route 53 Resolver DNS Firewall a uma VPC para filtrar consultas de DNS, o DNS Firewall começa a enviar métricas e dimensões uma vez a cada 5 minutos CloudWatch para aproximadamente as consultas que ele filtra. Para obter informações sobre as métricas e dimensões do DNS Firewall, consulte CloudWatch métricas para o Route 53 Resolver DNS Firewall.

Você pode usar os procedimentos a seguir para visualizar as métricas no CloudWatch console ou visualizá-las usando o AWS Command Line Interface (AWS CLI).

Para visualizar as métricas do DNS Firewall usando o console CloudWatch

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Na barra de navegação, escolha a região que você quer exibir.
3. No painel de navegação, selecione Métricas.
4. Na guia All metrics (Todas as métricas), selecione Route 53 Resolver (Resolvedor do Route 53).
5. Escolha uma métrica na qual esteja interessado.

Para visualizar métricas usando o AWS CLI

- Em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

Tópicos

- CloudWatch métricas para o Route 53 Resolver DNS Firewall

CloudWatch métricas para o Route 53 Resolver DNS Firewall

O namespace `AWS/Route53Resolver` inclui métricas para grupos de regras do Firewall DNS do Route 53 Resolver.

Tópicos

- Métricas para grupos de regras do Firewall DNS do Route 53 Resolver
- Métricas para VPCs
- Métricas para grupo de regras de firewall e associação de VPC
- Métricas para uma lista de domínios em um grupo de regras de firewall

Métricas para grupos de regras do Firewall DNS do Route 53 Resolver

FirewallRuleGroupQueryVolume

O número de consultas do Firewall DNS que correspondem a um grupo de regras de firewall (especificado por `FirewallRuleGroupId`).

Dimensões: `FirewallRuleGroupId`

Estatística válida: soma

Unidades: contagem

Métricas para VPCs

VpcFirewallQueryVolume

O número de consultas do Firewall DNS de uma VPC (especificado por `VpcId`).

Dimensões: `VpcId`

Estatística válida: soma

Unidades: contagem

Métricas para grupo de regras de firewall e associação de VPC

FirewallRuleGroupVpcQueryVolume

O número de consultas do Firewall DNS de uma VPC (especificado por `VpcId`) que correspondem a um grupo de regras de firewall (especificado por `FirewallRuleGroupId`).

Dimensões: `FirewallRuleGroupId, VpcId`

Estatística válida: soma

Unidades: contagem

Métricas para uma lista de domínios em um grupo de regras de firewall

FirewallRuleQueryVolume

O número de consultas de firewall DNS que correspondem a uma lista de domínios de firewall (especificado por `FirewallDomainListId`) dentro de um grupo de regras de firewall (especificado por `FirewallRuleGroupId`).

Dimensões: `FirewallRuleGroupId, FirewallDomainListId`

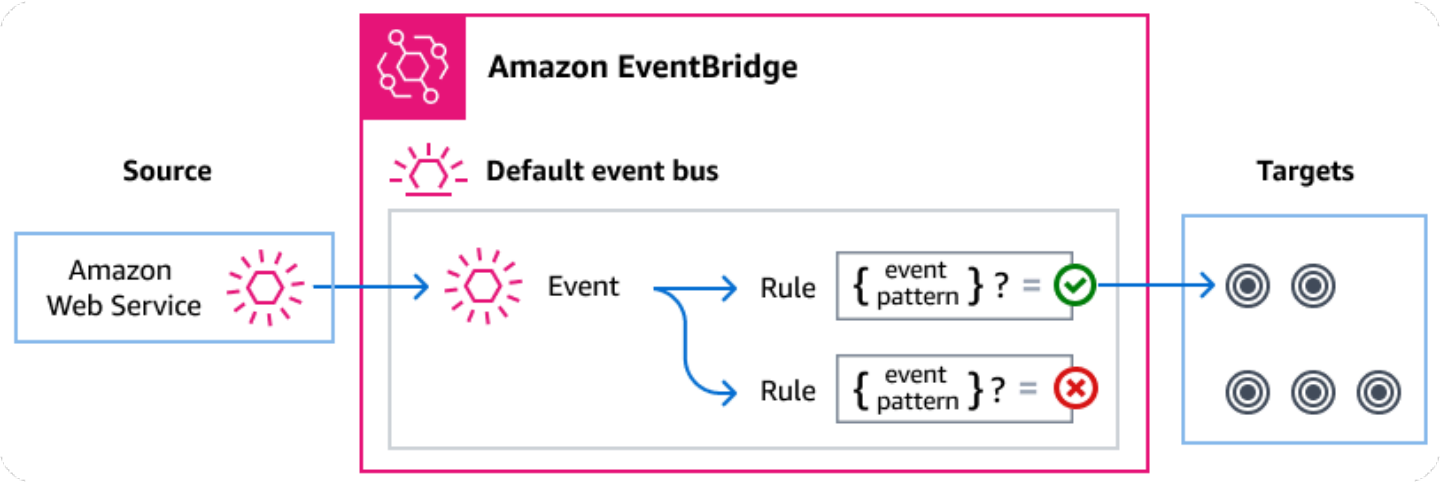
Estatística válida: soma

Unidades: contagem

Gerenciando eventos do Route 53 Resolver DNS Firewall usando Amazon EventBridge

Amazon EventBridge é um serviço sem servidor que usa eventos para conectar componentes do aplicativo, facilitando a criação de aplicativos escaláveis orientados por eventos. A arquitetura orientada por eventos é um estilo de criação de sistemas de software com acoplamento fraco que funcionam juntos emitindo e respondendo a eventos. Os eventos representam uma mudança em um recurso ou ambiente.

Como acontece com muitos AWS serviços, o DNS Firewall gera e envia eventos para o barramento de eventos EventBridge padrão. (O barramento de eventos padrão é provisionado automaticamente em cada conta da AWS .) Um barramento de eventos é um roteador que recebe eventos e os entrega a zero ou mais destinos, ou alvos. As regras especificadas para o barramento de eventos avaliam os eventos à medida que eles chegam. Cada regra verifica se um evento corresponde ao padrão do evento. Se o evento corresponder, o barramento de eventos enviará o evento para os destinos especificados.



Tópicos

- Eventos do Route 53 Resolver DNS Firewall
- Enviando eventos do Route 53 Resolver DNS Firewall usando regras EventBridge
- Amazon EventBridge permissões
- EventBridge Recursos adicionais
- Referência de detalhes de eventos do Route 53 Resolver DNS Firewall

Eventos do Route 53 Resolver DNS Firewall

O Resolvedor do Route 53 envia eventos do DNS Firewall para o barramento de EventBridge eventos padrão automaticamente. Você pode criar regras no barramento de eventos; cada regra inclui um padrão de evento e um ou mais alvos. Os eventos que correspondem ao padrão de eventos de uma regra são entregues aos alvos especificados com base no melhor esforço. Os eventos podem ser entregues fora de ordem.

Os eventos a seguir são gerados pelo DNS Firewall. Para obter mais informações, consulte EventBridgeo Guia Amazon EventBridge do usuário. .

Tipo de detalhe do evento	Descrição
Bloco de firewall DNS	Qualquer ação de bloqueio executada em um domínio.
Alerta de firewall de DNS	Qualquer ação de alerta executada em um domínio.

Enviando eventos do Route 53 Resolver DNS Firewall usando regras EventBridge

Para que o barramento de eventos EventBridge padrão envie eventos do Firewall DNS para um destino, você deve criar uma regra que contenha um padrão de eventos que corresponda aos dados nos eventos do Firewall DNS desejados.

A criação de uma regra consiste nas seguintes etapas gerais:

1. Criar um padrão de evento para a regra que especifica:
   - O Route 53 Resolver é a fonte dos eventos que estão sendo avaliados pela regra.
   - (Opcional): qualquer outro dado de evento para comparar.

   Para mais informações, consulte ???.
2. (Opcional): Criação de um transformador de entrada que personaliza os dados do evento antes de EventBridge passar as informações para o destino da regra.

   Para obter mais informações, consulte Transformação da entrada no Guia do usuário do EventBridge .
3. Especificar o (s) destino (s) para o (s) qual (is) você EventBridge deseja entregar eventos que correspondam ao padrão do evento.

   Os destinos podem ser outros AWS serviços, aplicativos software-as-a-service (SaaS), destinos de API ou outros endpoints personalizados. Para obter mais informações, consulte Targets (Alvos) no Guia do usuário do EventBridge .

Para obter instruções abrangentes de como criar regras de barramento de eventos, consulte Criar regras que reagem a eventos no Guia do usuário do EventBridge .

Criação de padrões de eventos para eventos do Route 53 Resolver DNS Firewall

Quando o DNS Firewall entrega um evento ao barramento de eventos padrão, EventBridge usa o padrão de evento definido para cada regra para determinar se o evento deve ser entregue ao (s) alvo (s) da regra. Um padrão de evento corresponde aos dados nos eventos do Firewall DNS desejados. Cada padrão de evento é um objeto JSON que contém:

- Um atributo `source` que identifica o serviço que envia o evento. Para eventos do DNS Firewall, a origem é `aws.route53resolver`.

- (Opcional): um atributo `detail-type` que contém uma matriz dos tipos de eventos a serem correlacionados.
- (Opcional): um atributo `detail` que contém quaisquer outros dados relacionados aos eventos a serem correlacionados.

Por exemplo, o padrão de eventos a seguir corresponde aos eventos de alerta e bloqueio do Firewall DNS:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

Embora o seguinte padrão de evento corresponda a uma ação BLOCK:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

O Firewall DNS envia o mesmo evento para o mesmo domínio somente uma vez em uma janela de 6 horas. Por exemplo: .

1. A instância i-123 enviou uma consulta de DNS exampledomain.com no momento T1. O Firewall DNS envia um alerta ou evento de bloqueio, pois essa é a primeira ocorrência.
2. A instância i-123 enviou uma consulta DNSQuery exampledomain.com no tempo T1+30 minutos. O Firewall DNS não envia um alerta nem bloqueia um evento, pois essa é uma ocorrência repetida dentro da janela de 6 horas.
3. A instância i-123 enviou uma consulta de DNS exampledomain.com no horário T1+7 horas. O Firewall DNS envia um alerta ou evento de bloqueio quando isso ocorre fora da janela de 6 horas.

Para obter mais informações sobre como escrever padrões de eventos, consulte Padrões de eventos no Guia do usuário do EventBridge .

Testando padrões de eventos para eventos do DNS Firewall em EventBridge

Você pode usar o EventBridge Sandbox para definir e testar rapidamente um padrão de evento, sem precisar concluir o processo maior de criação ou edição de uma regra. Usando o Sandbox,

você pode definir um padrão de evento e usar um evento de amostra para confirmar se o padrão corresponde aos eventos desejados. EventBridge oferecem a opção de criar uma nova regra usando esse padrão de evento, diretamente da sandbox.

Para obter mais informações, consulte Testando um padrão de evento usando o EventBridge Sandbox no Guia do EventBridge usuário.

Criando uma EventBridge regra e um destino para o Firewall DNS

O procedimento a seguir mostra como criar uma regra que permite EventBridge enviar eventos para todas as ações de alerta e bloqueio do Firewall DNS e adicionar uma AWS Lambda função como destino para a regra.

1. Use AWS CLI para criar uma EventBridge regra:

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. Anexe uma função Lambda como destino para a regra:

```
AWS events put-targets --rule dns-firewall-rule --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

3. Para adicionar as permissões necessárias para invocar o destino, execute o seguinte comando do AWS CLI Lambda:

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Amazon EventBridge permissões

O Firewall do DNS não exige nenhuma permissão adicional para entregar eventos a. Amazon EventBridge

Talvez os destinos que você especificar precisem de determinadas permissões ou configurações. Para obter mais detalhes sobre o uso de serviços específicos para destinos, consulte Destinos do Amazon EventBridge no Amazon EventBridge Guia do usuário do .

EventBridge Recursos adicionais

Consulte os tópicos a seguir no Guia do Amazon EventBridge usuário para obter mais informações sobre como usar EventBridge para processar e gerenciar eventos.

- Para obter informações detalhadas sobre como os barramentos de eventos funcionam, consulte Barramento de eventos do Amazon EventBridge.
- Para obter informações sobre a estrutura de eventos, consulte Eventos
- Para obter informações sobre a construção de padrões de eventos EventBridge para uso ao comparar eventos com regras, consulte Padrões de eventos.
- Para obter informações sobre a criação de regras para especificar quais eventos são processados pelo EventBridge , consulte Regras.
- Para obter informações sobre como especificar para quais serviços ou outros destinos EventBridge enviam eventos correspondentes, consulte Targets.

Referência de detalhes de eventos do Route 53 Resolver DNS Firewall

Todos os eventos dos AWS serviços têm um conjunto comum de campos contendo metadados sobre o evento, como o AWS serviço que é a origem do evento, a hora em que o evento foi gerado, a conta e a região em que o evento ocorreu e outros. Para obter as definições desses campos gerais, consulte Referência da estrutura de eventos no Guia do usuário do Amazon EventBridge .

Além disso, cada evento tem um campo de `detail` que contém dados específicos desse determinado evento. A referência abaixo define os campos de detalhes dos vários eventos do DNS Firewall.

Ao usar EventBridge para selecionar e gerenciar eventos do DNS Firewall, é útil ter em mente o seguinte:

- O `source` campo para todos os eventos do DNS Firewall está definido como. `aws.route53resolver`
- O campo do `detail-type` especifica o tipo de evento.

  Por exemplo, o `DNS Firewall Block` ou o `DNS Firewall Alert`.
- O campo de `detail` contém os dados específicos desse determinado evento.

Para obter informações sobre a criação de padrões de eventos que permitem que as regras correspondam aos eventos do Firewall DNS, consulte Padrões de eventos no Guia do Amazon EventBridge usuário.

Para obter mais informações sobre eventos e como EventBridge os processa, consulte Amazon EventBridge eventos no Guia Amazon EventBridge do usuário.

Tópicos

Detalhe do evento de alerta do DNS Firewall

Abaixo estão os campos de detalhes do evento de status do alerta.

Os `detail-type` campos `source` e estão incluídos porque contêm valores específicos para eventos do 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",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
```

```
        "id": "string"
      }
    }
]
```

`detail-type`

Identifica o tipo de evento.

Para esse evento, esse valor é`DNS Firewall Alert`.

`source`

Identifica o serviço que gerou o evento. Para eventos de firewall de DNS, esse valor é`aws.route53resolver`.

`detail`

Um objeto JSON contém informações sobre o evento. O serviço que gera o evento determina o conteúdo desse campo.

Para esse evento, esses dados incluem:

`account-id`

O ID do Conta da AWS que criou a VPC.

`last-observed-at`

A data e hora de quando a consulta de alerta/bloqueio foi feita na VPC.

`query-name`

O nome de domínio (example.com) ou de subdomínio (www.example.com) especificado na consulta.

`query-type`

O tipo de registro DNS especificado na solicitação ou QUALQUER. Para obter informações sobre os tipos com suporte do Route 53, consulte Tipos de registro de DNS com suporte.

`query-class`

A classe da consulta.

`transport`

O protocolo usado para enviar a consulta de DNS.

`firewall-rule-action`

A ação especificada pela regra que correspondeu ao nome de domínio na consulta. `ALERT` ou `BLOCK`.

`firewall-rule-group-id`

O ID do grupo de regras do Firewall DNS que correspondeu ao nome de domínio na consulta. Para obter mais informações sobre os grupos de regras de firewall, consulte Firewall Regras e grupos de regras do Firewall DNS DNS.

`firewall-domain-list-id`

A lista de domínios usada pela regra que correspondeu ao nome de domínio na consulta.

`resourcese`

Contém tipos de recursos e detalhes adicionais sobre eles.

`resource-type`

Especifica o tipo de recurso, como o endpoint do resolvedor ou uma instância de VPC.

`resource-type``-detail`

Detalhes adicionais sobre o recurso.

Example Evento de alerta do DNS Firewall

Veja a seguir um exemplo de evento de alerta.


```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
```

```
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```

Detalhe do evento de bloqueio do firewall DNS

Abaixo estão os campos de detalhes do *`nome do evento`*.

Os `detail-type` campos `source` e estão incluídos porque contêm valores específicos para eventos do 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",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

Identifica o tipo de evento.

Para esse evento, esse valor é`DNS Firewall Alert`.

`source`

Identifica o serviço que gerou o evento. Para eventos de firewall de DNS, esse valor é`aws.route53resolver`.

`detail`

Um objeto JSON contém informações sobre o evento. O serviço que gera o evento determina o conteúdo desse campo.

Para esse evento, esses dados incluem:

`account-id`

O ID do Conta da AWS que criou a VPC.

`last-observed-at`

A data e hora de quando a consulta de alerta/bloqueio foi feita na VPC.

`query-name`

O nome de domínio (example.com) ou de subdomínio (www.example.com) especificado na consulta.

`query-type`

O tipo de registro DNS especificado na solicitação ou QUALQUER. Para obter informações sobre os tipos com suporte do Route 53, consulte Tipos de registro de DNS com suporte.

`query-class`

A classe da consulta.

`transport`

O protocolo usado para enviar a consulta de DNS.

`firewall-rule-action`

A ação especificada pela regra que correspondeu ao nome de domínio na consulta. `ALERT` ou `BLOCK`.

`firewall-rule-group-id`

O ID do grupo de regras do Firewall DNS que correspondeu ao nome de domínio na consulta. Para obter mais informações sobre os grupos de regras de firewall, consulte Firewall Regras e grupos de regras do Firewall DNS DNS.

`firewall-domain-list-id`

A lista de domínios usada pela regra que correspondeu ao nome de domínio na consulta.

`resourcese`

Contém tipos de recursos e detalhes adicionais sobre eles.

`resource-type`

Especifica o tipo de recurso, como o endpoint do resolvedor ou uma instância de VPC.

`resource-type``-detail`

Detalhes adicionais sobre o recurso.

Example Evento de exemplo

Veja a seguir um exemplo de evento de bloco.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
```

```
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```


Registro de chamadas de API do Amazon Route 53 com AWS CloudTrail

O Route 53 é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Route 53. CloudTrail captura todas as chamadas de API para o Route 53 como eventos, incluindo chamadas do console do Route 53 e de chamadas de código para as APIs do Route 53. Se você criar uma trilha, poderá habilitar a entrega

contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Route 53. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita para o Route 53, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Tópicos

Informações sobre o Route 53 em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Route 53, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Route 53, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Route 53 são registradas CloudTrail e documentadas na Referência de API do Amazon Route 53. Por exemplo, chamadas para as `RegisterDomain` ações `CreateHostedZone` `CreateHealthCheck`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias para um perfil ou usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

Como visualizar eventos do Route 53 no histórico de eventos

CloudTrail permite que você visualize eventos recentes no histórico de eventos. Para visualizar os eventos de solicitações da API do Route 53, você deve escolher US East (N. Virginia) (Leste dos EUA [Norte da Virgínia]) no seletor de região na parte superior do console. Para obter mais informações, consulte Visualização de CloudTrail eventos com histórico de eventos no Guia AWS CloudTrail do usuário.

Noções básicas sobre entradas de arquivos de log do Route 53

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O elemento `eventName` identifica a ação que ocorreu. (Nos CloudTrail registros, a primeira letra é minúscula para ações de registro de domínio, embora esteja em maiúscula nos nomes das ações. Por exemplo, `UpdateDomainContact` aparece como `updateDomainContact` nos registros). CloudTrail suporta todas as ações da API do Route 53. O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra as seguintes ações:

- Listar as zonas hospedadas associadas a uma AWS conta
- Criar uma verificação de integridade
- Criar dois registros
- Excluir uma zona hospedada

- Atualizar informações de um domínio registrado
- Criar um endpoint de saída do 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"
        }
    ]
}
```

Solução de problemas do Amazon Route 53

Os tópicos deste capítulo podem ajudá-lo a solucionar problemas com o seu registro de domínio e configuração de DNS.

Tópicos

Meu domínio não está disponível na Internet

Aqui estão os motivos mais comuns para o seu domínio não estar disponível na Internet.

Tópicos

Você registrou um novo domínio, mas não clicou no link no e-mail de confirmação

Quando você registra um novo domínio, a ICANN exige uma confirmação de que o endereço de e-mail de contato do registrante é válido. Para obter a confirmação, enviamos um e-mail que contém um link. (Se você não responder ao primeiro e-mail, reenviamos o mesmo e-mail mais duas vezes.) Você tem entre 3 e 15 dias para clicar no link, dependendo do domínio de nível superior. Depois desse período, o link deixa de funcionar.

Se você não clicar no link do e-mail no tempo alocado, a ICANN exigirá que o domínio seja suspenso. Para obter informações sobre como reenviar o e-mail de confirmação para o contato do registrante, consulte Reenviar e-mails de confirmação e autorização.

Você transferiu o registro de domínio ao Amazon Route 53, mas não transferiu o serviço DNS

Se o registrador anterior ofereceu o serviço DNS gratuitamente com o registro de domínio, ele pode ter interrompido o fornecimento do serviço DNS quando você transferiu o registro de domínio para o Route 53. Execute o procedimento a seguir para determinar se esse é o problema e, se esse for o caso, resolvê-lo.

Para restaurar o serviço DNS se o registrador anterior o tiver cancelado após a transferência de registro de domínio para o Route 53

1. Entre em contato com o registrador anterior e confirme se ele cancelou o serviço de DNS do seu domínio. Se esse for o caso, aqui estão as três formas mais rápidas de restaurar o serviço de DNS do domínio, em ordem de preferência:

   - Se o registrador anterior fornece serviço de DNS pago, peça que ele restaure o serviço usando os registros de DNS e os servidores de nome antigos de seu domínio.
   - Se o registrador anterior não fornece serviço de DNS pago sem registro de domínio, pergunte se você pode transferir o registro de domínio de volta para ele e faça com que ele restaure o serviço de DNS, usando os registros de DNS e os servidores de nome antigos do seu domínio.
   - Se você puder transferir o registro de domínio de volta para o registrador anterior, mas se ele não tiver mais seus registros de DNS, pergunte se é possível transferir o registro de domínio de volta para ele e obter o mesmo conjunto de servidores de nome atribuído anteriormente ao

domínio. Se isso for possível, você mesmo terá que recriar seus registros de DNS antigos. No entanto, assim que você fizer isso, seu domínio estará disponível novamente.

Se o registrador anterior não puder ajudar com qualquer uma dessas opções, vá para a etapa 2.

> **Important**
>
> Se você não puder restaurar o serviço DNS usando os servidores de nome especificados quando seu domínio foi transferido para o Route 53, talvez você precise aguardar até dois dias após a conclusão das etapas restantes neste procedimento para que o domínio volte a ficar disponível na Internet. Normalmente, os resolvedores de DNS armazenam em cache os servidores de nome de um domínio por 24 a 48 horas. Esse é o tempo necessário para que todos os resolvedores de DNS obtenham os nomes dos novos servidores de nome.

2. Escolha um novo serviço DNS, por exemplo, o Route 53.
3. Usando o método fornecido pelo novo serviço de DNS, crie uma zona hospedada e os registros:

   a. Crie uma zona hospedada que tenha o mesmo nome que o seu domínio, como exemplo.com.

   b. Use o arquivo de zona que você obteve do registrador anterior para criar registros.

   Se você escolheu o Route 53 como o novo serviço DNS, você poderá criar registros importando o arquivo de zona. Para ter mais informações, consulte Criar registros importando um arquivo de zona.
4. Obtenha os servidores de nome da nova zona hospedada. Se você tiver escolhido o Route 53 como o serviço DNS, consulte Obter os servidores de nome de uma zona hospedada pública.
5. Altere os servidores de nome de seu domínio para os servidores de nome que você obteve na etapa 4. Para ter mais informações, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.

Você transferiu o registro de domínio e especificou os servidores de nome incorretos nas configurações de domínio

Quando você transfere o registro de domínio ao Amazon Route 53, uma das configurações que deve ser especificada para o domínio é o conjunto de servidores de nomes que responderá a consultas de DNS desse domínio. Esses servidores de nome vêm da zona hospedada que tem o mesmo nome que o domínio. A zona hospedada contém informações sobre como você deseja rotear o tráfego para o domínio, tal como o endereço IP de um servidor web para www.exemplo.com.

Talvez você tenha acidentalmente especificado os servidores de nome para a zona hospedada incorreta, o que é especialmente fácil se você tiver mais de uma zona hospedada que tenha o mesmo nome que o domínio. Para confirmar que o domínio está usando os servidores de nome para a zona hospedada correta e, se necessário, atualizar os servidores de nome do domínio, execute os procedimentos a seguir.

> **Important**
>
> Se você especificou os registros do servidor de nome incorretos quando transferiu o domínio para o Route 53, o serviço DNS poderá levar até dois dias para ser totalmente restaurado depois que você corrigir os servidores de nome do domínio. Isso ocorre porque os resolvedores de DNS na Internet costumam solicitar os servidores de nome apenas uma vez a cada dois dias e armazenam a resposta em cache.

Para obter os servidores de nome da sua zona hospedada

1. Se você estiver usando outro serviço de DNS para o domínio, use o método fornecido pelo serviço de DNS para obter os servidores de nome da zona hospedada. Em seguida, vá para o procedimento seguinte.

   Se você estiver usando o Route 53 como serviço DNS para o domínio, faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Zonas hospedadas, marque o botão circular (não o nome) para a zona hospedada.

> **Important**
>
> Se você tiver mais de uma zona hospedada com o mesmo nome, certifique-se de que esteja recebendo os servidores de nome da zona hospedada correta.

4. No painel direito, anote os quatro servidores listados para Servidores de nomes.

Para confirmar que o domínio está usando os servidores de nome corretos

1. Se você estiver usando outro serviço DNS para o domínio, faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/

   Se você estiver usando o Route 53, vá para a próxima etapa.
2. No painel de navegação, escolha Domínios registrados.
3. Escolha o nome do domínio para o qual você deseja editar as configurações.
4. Escolha Adicionar ou editar servidores de nome.
5. Compare a lista de servidores de nome que você obteve no procedimento anterior com os servidores de nome listados na caixa de diálogo Editar servidores de nome para nome do domínio.
6. Se os servidores de nome listados aqui não corresponderem aos servidores de nome que você obteve no procedimento anterior, altere os servidores de nome aqui e, em seguida, escolha Atualizar.

Você transferiu o serviço de DNS primeiro, mas não esperou o tempo suficiente antes de transferir o registro de domínio

Quando transferiu o serviço DNS para o Amazon Route 53 ou outro serviço, você atualizou a configuração do seu domínio junto ao registrador de domínio para usar os servidores de nome do novo serviço DNS.

Os resolvedores de DNS, que respondem a solicitações para seu domínio, normalmente armazenam em cache os nomes de servidores de nome por 24 a 48 horas. Se você alterar o serviço de DNS de um domínio e substituir os servidores de nome de um serviço de DNS pelos servidores de nome de outro serviço de DNS, pode levar até 48 horas antes que os resolvedores de DNS comecem a usar os novos servidores de nome e; portanto, o novo serviço de DNS.

Veja como transferir seu serviço de DNS e transferir seu domínio logo em seguida pode fazer com que o domínio fique indisponível na Internet:

1. Você transferiu o serviço de DNS de seu domínio.
2. Você transferiu seu domínio para o Route 53 antes que os resolvedores de DNS começassem a usar os servidores de nome do novo serviço DNS.
3. O registrador anterior cancelou o serviço DNS de seu domínio assim que o domínio foi transferido para o Route 53.
4. Os resolvedores de DNS ainda estão roteando consultas para seu serviço de DNS antigo, mas não há mais registros que informam como rotear o tráfego.

Quando o armazenamento em cache expirar para os servidores de nome do serviço de DNS antigo, o DNS começará a usar o novo serviço de DNS. Infelizmente, não é possível acelerar esse processo.

Você excluiu a zona hospedada que o Route 53 está usando para encaminhar o tráfego de Internet do domínio

Se o Route 53 for o serviço DNS para seu domínio e, se você excluir a zona hospedada que é usada para encaminhar o tráfego de Internet para o domínio, o domínio não estará mais disponível na Internet. Isso se aplica independentemente de o domínio estar registrado no Route 53.

> **Important**
>
> A restauração do serviço de Internet para o domínio pode levar até 48 horas.

Para restaurar o serviço de Internet se você excluir uma zona hospedada que o Route 53 está usando para encaminhar o tráfego de Internet de um domínio

1. Crie outra obter zona hospedada com o mesmo nome do domínio. Para ter mais informações, consulte Criar uma zona hospedada pública.
2. Recrie os registros que estavam na zona hospedada que você excluiu. Para ter mais informações, consulte Trabalhar com registros.
3. Obtenha os nomes dos servidores que o Route 53 atribuiu à nova zona hospedada. Para ter mais informações, consulte Obter os servidores de nome de uma zona hospedada pública.
4. Atualize o registro de domínio para usar os servidores de nome obtidos na etapa 3.

- Se o domínio estiver registrado no Route 53, consulte Adicionar ou alterar servidores de nome e registros cola de um domínio.
- Se o domínio estiver registrado em outro registrador de domínios, use o método fornecido pelo registrador para atualizar o registro de domínios e usar os novos servidores de nome.

5. Aguarde até que o TTL dos servidores de nome passe pelos resolvedores recursivos que armazenaram em cache os nomes dos servidores da zona hospedada excluída. Depois que o TTL passar, quando um navegador ou aplicação enviar uma consulta de DNS para o domínio ou um de seus subdomínios, um resolvedor recursivo encaminhará a consulta aos servidores de nome do Route 53 referentes à nova zona hospedada. Para ter mais informações, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

   O TTL dos servidores de nome podem ter até 48 horas de duração, dependendo do TLD do domínio.

O seu domínio foi suspenso

Seu domínio pode estar indisponível na Internet, pois tivemos que suspendê-lo. Para ter mais informações, consulte Meu domínio está suspenso (o status é ClientHold).

Meu domínio está suspenso (o status é ClientHold)

Se o Amazon Route 53 suspender o domínio, o domínio se tornará indisponível na Internet. Você pode usar um dos seguintes métodos para determinar se um domínio foi suspenso:

- Na página Registered domains (Domínios registrados) do console do Route 53, localize o nome do domínio na tabela Alerts (Alertas) na parte inferior da página. Se o valor da coluna Status for clientHold, o domínio foi suspenso.
- Envie uma consulta WHOIS para o domínio. Se o valor da coluna Status do domínio for clientHold, o domínio foi suspenso. O comando WHOIS está disponível em muitos sistemas operacionais e também como um aplicativo web em muitos sites.

Além disso, quando suspendemos um domínio, geralmente enviamos um e-mail para o endereço de e-mail de contato do registrante do domínio. No entanto, se o domínio foi suspenso com base em uma ordem judicial, a justiça pode não permitir que notifiquemos o contato do registrante.

Para tornar um domínio disponível na Internet novamente, você deve cancelar a suspensão dele. Aqui estão os motivos pelos quais um domínio pode ser suspenso e como você pode cancelar a suspensão dele.

> **Note**
>
> Se precisar de ajuda para cancelar a suspensão do seu domínio, entre em contato com o AWS Support gratuitamente. Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Tópicos

Você registrou um novo domínio, mas não clicou no link no e-mail de confirmação

Quando você registra um domínio pela primeira vez, a ICANN exige que recebamos a confirmação de que o endereço de e-mail do contato do solicitante do registro é válido. AWS Para obter a confirmação, enviamos um e-mail que contém um link. Você tem entre 3 e 15 dias para clicar no link, dependendo do domínio de nível superior. Depois desse período, o link deixa de funcionar.

> **Note**
>
> Se você já registrou um ou mais domínios com o Amazon Route 53 e usou o mesmo endereço de e-mail de contato para o registrante, não enviaremos um e-mail de confirmação.

Se você não clicar no link do e-mail no tempo alocado, a ICANN exigirá que o domínio seja suspenso. Para obter informações sobre como reenviar o e-mail de confirmação para o contato do

registrante, consulte Reenviar e-mails de confirmação e autorização. Quando você confirmar que o endereço de e-mail é válido, cancelaremos automaticamente a suspensão do domínio.

Você desabilitou a renovação automática do domínio e o domínio expirou

Quando a renovação automática é habilitada para um domínio (o valor padrão de um domínio novo ou transferido), renovamos automaticamente o registro do domínio pouco antes da data de expiração. Se você desabilitar a renovação automática, enviamos três e-mails de lembrete, informando que o registro de domínio está prestes a expirar, para o endereço de e-mail de contato do registrante. Começamos a enviar esses e-mails 45 dias antes da expiração do domínio.

Se você desabilitar a renovação automática do domínio e não estender manualmente o período de registro do domínio, em geral, suspenderemos o domínio na data de expiração. Observe que os registros de alguns domínios excluem o domínio mesmo antes da data de expiração.

Para obter informações sobre como renovar um domínio expirado, consulte Renovação do registro de um domínio.

Você alterou o endereço de e-mail do contato registrante, mas não verificou se o novo endereço de e-mail é válido

Se você alterar o endereço de e-mail do contato registrante para um endereço que ainda não foi verificado, a ICANN exigirá uma confirmação de que o endereço de e-mail do contato registrante é válido. Para obter a confirmação, enviamos um e-mail que contém um link. Você tem entre 3 e 15 dias para clicar no link, dependendo do domínio de nível superior. Depois desse período, o link deixa de funcionar.

Se você não clicar no link do e-mail no tempo permitido pelo registro do TLD, a ICANN exigirá que o domínio seja suspenso. Para obter informações sobre como reenviar o e-mail de confirmação para o contato do registrante, consulte Reenviar e-mails de confirmação e autorização. Quando você confirmar que o endereço de e-mail é válido, cancelaremos automaticamente a suspensão do domínio.

Não foi possível processar o pagamento da renovação automática do domínio e o domínio expirou

Se a renovação automática estiver habilitada para um domínio, mas não foi possível processar o pagamento (por exemplo, porque seu cartão de crédito expirou), enviaremos vários e-mails para o endereço de e-mail de contato do registrante do domínio. Se não recebermos o pagamento,

suspenderemos o domínio na data de expiração. Observe que os registros de alguns domínios excluem o domínio mesmo antes da data de expiração.

Para obter informações sobre como renovar um domínio expirado, consulte Renovação do registro de um domínio.

Suspendemos o domínio devido a uma violação da política de uso aceitável da AWS

Se suspendermos um domínio devido a uma violação da política de uso aceitável da AWS, enviaremos uma notificação por e-mail para o contato do registrante do domínio. (Não enviamos um e-mail de notificação se a AWS conta já estiver suspensa por fraude.)

Para contestar uma suspensão, envie um e-mail para abuse@amazon.com.

Suspendemos o domínio devido a uma ordem judicial

Se um domínio está suspenso como resultado de uma ordem judicial, não podemos cancelar a suspensão do domínio até que a ordem judicial tenha sido revogada. Para contestar a validade de uma ordem judicial, envie um e-mail para abuse@amazon.com e anexe os documentos aplicáveis.

A transferência do meu domínio para o Amazon Route 53 falhou

Aqui estão alguns motivos comuns pelos quais a transferência de um domínio para o Amazon Route 53 falha.

Tópicos

- Você não clicou no link no e-mail de autorização
- O código de autorização que você obteve do registrador atual não é válido
- Erro “Parameters in request are not valid” (Parâmetros inválidos na solicitação) ao tentar transferir um domínio .es para o Amazon Route 53
- O nome de domínio internacionalizado que você está transferindo para o Amazon Route 53 está listado em punycode?

Você não clicou no link no e-mail de autorização

Quando você transfere o registro do domínio ao Amazon Route 53, a ICANN, órgão que rege o registro de domínios, nos obriga a obter autorização para a transferência junto ao contato do

registrante desse domínio. Para obter a autorização, enviamos a você um e-mail que contém um link. Você tem entre 5 e 15 dias para clicar no link, dependendo do domínio de nível superior. Depois desse período, o link deixa de funcionar.

Se você não clicar no link do e-mail no tempo alocado, a ICANN exigirá que cancelemos a transferência. Para obter informações sobre como reenviar o e-mail de autorização para o contato do registrante, consulte Reenviar e-mails de confirmação e autorização.

O código de autorização que você obteve do registrador atual não é válido

Se você solicitar a transferência de um domínio para o Amazon Route 53 e não receber o e-mail de autorização, verifique a página de status no console do Route 53. Se a página de status mostra que o código de autorização de transferência que você recebeu do registrador não é válido, siga estas etapas:

1. Entre em contato com o registrador atual do domínio e solicite um novo código de autorização. Confirme o seguinte:
   - Por quanto tempo o novo código de autorização permanecerá ativo. Você deve solicitar uma transferência de domínio antes que o código expire.
   - O novo código de autorização é diferente do código que não é válido. Caso contrário, peça ao registrador atual para atualizar o código de autorização.
2. Envie outra solicitação para transferir o domínio. Para obter mais informações, consulte Etapa 5: solicitar a transferência no tópico Como transferir registro de um domínio para o Amazon Route 53.

Erro “Parameters in request are not valid” (Parâmetros inválidos na solicitação) ao tentar transferir um domínio .es para o Amazon Route 53

O Amazon Route 53 retorna um erro “Parameters in request are not valid” (Parâmetros inválidos na solicitação) quando você tenta transferir um domínio .es para o Route 53, e o tipo de contato do registrante é Company (Empresa). Para concluir a transferência, altere o tipo de contato do solicitante para Person (Pessoa) e reenvie.

O nome de domínio internacionalizado que você está transferindo para o Amazon Route 53 está listado em punycode?

Ao registrar um novo nome de domínio ou criar zonas hospedadas e registros, você pode especificar letras diferentes de a-z (por exemplo, o ç em França), caracteres em outros alfabetos (por exemplo, cirílico ou árabe) e caracteres em chinês, japonês ou coreano. O Amazon Route 53 armazena esses nomes de domínio internacionalizados (IDNs) em Punycode, que representa caracteres Unicode como strings ASCII.

Se você receber um erro ao transferir um IDNs para o Route 53, use punycode para representá-lo e tente novamente. Para ter mais informações, consulte Formatar nomes de domínio internacionalizados.

Alterei as configurações de DNS, mas elas não entraram em vigor

Se você alterou as configurações de DNS, aqui estão alguns motivos comuns pelos quais as alterações não entraram em vigor.

Tópicos

- Você transferiu o serviço DNS para o Amazon Route 53 nas últimas 48 horas; portanto, o DNS ainda está usando o serviço DNS anterior
- Recentemente, você transferiu o serviço DNS para o Amazon Route 53, mas não atualizou os servidores de nomes junto ao registrador de domínio
- Os resolvedores de DNS ainda estão usando as configurações antigas do registro
- Você tem mais de uma zona hospedada com o mesmo nome e atualizou a que não está associada ao domínio

Você transferiu o serviço DNS para o Amazon Route 53 nas últimas 48 horas; portanto, o DNS ainda está usando o serviço DNS anterior

Quando você transferiu o serviço DNS ao Amazon Route 53, você usou o método fornecido pelo registrador do seu domínio para substituir os servidores de nomes do serviço DNS anterior pelos quatro servidores de nomes do Route 53.

> **Note**
>
> Se você não tiver certeza de que fez essa parte, consulte Recentemente, você transferiu o serviço DNS para o Amazon Route 53, mas não atualizou os servidores de nomes junto ao registrador de domínio.

Normalmente, os registradores de domínio usam um TTL (tempo de vida) de 24 a 48 horas para servidores de nome. Isso significa que quando um resolvedor de DNS obtém os servidores de nome para seu domínio, ele usa essas informações por até 48 horas antes de enviar outra solicitação para os servidores de nome atuais do domínio. Se você transferiu o serviço DNS para o Route 53 nas últimas 48 horas e alterou as configurações DNS, alguns resolvedores de DNS ainda estão usando o serviço DNS antigo para encaminhar o tráfego para o domínio.

Recentemente, você transferiu o serviço DNS para o Amazon Route 53, mas não atualizou os servidores de nomes junto ao registrador de domínio

O registrador do seu domínio tem uma variedade de informações sobre o domínio, incluindo os servidores de nome do serviço de DNS do domínio. Normalmente, o registrador de domínio também é o seu serviço de DNS; portanto, os servidores de nome associados ao domínio pertencem ao registrador. Esses servidores de nome informam ao DNS onde obter informações sobre como você deseja rotear o tráfego do seu domínio, por exemplo, para o endereço IP de um servidor web do seu domínio.

Ao transferir o serviço DNS ao Amazon Route 53, você precisa usar o método fornecido pelo registrador do domínio para alterar os servidores de nomes associados a esse domínio. Geralmente, você está substituindo os servidores de nome fornecidos pelo registrador pelos quatro servidores de nome do Route 53 que estão associados à zona hospedada que você criou para o domínio.

Se você criou uma nova zona hospedada e registros para o seu domínio, e especificou configurações diferentes daquelas usadas para o serviço de DNS anterior, e se o DNS ainda está roteando tráfego para os recursos antigos, é possível que você não tenha atualizado os servidores de nome com o registrador de domínio. Para determinar se o registrador está usando os servidores de nome para sua zona hospedada do Route 53 e, se necessário, atualizar os servidores de nome do domínio, execute o procedimento a seguir:

Para obter os servidores de nome da sua zona hospedada e atualizar a configuração do servidor de nome junto ao registrador de domínio

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. No painel de navegação, escolha Zonas hospedadas.
3. Na página Hosted Zones (Zonas hospedadas), marque o botão circular (não o nome) para a zona hospedada.

   > **Important**
   >
   > Se você tiver mais de uma zona hospedada com o mesmo nome, certifique-se de que esteja recebendo os servidores de nome da zona hospedada correta.

4. Na lista Record name (Nome do registro), anote os quatro servidores listados para Name Servers (Servidores de nomes).
5. Usando o método fornecido pelo registrador do domínio, exiba a lista de servidores de nome do domínio.
6. Se os servidores de nome do domínio correspondem aos servidores de nome que você obteve na etapa 4, então a configuração do domínio está correta.

   Se os servidores de nome do domínio não corresponderem aos servidores de nome que você obteve na etapa 4, atualize o domínio para usar os servidores de nome do Route 53.
7.

> **Important**
>
> Quando você altera os servidores de nome do domínio para os servidores de nome de sua zona hospedada do Route 53, pode levar até dois dias para a alteração entrar em vigor e para o Route 53 se tornar seu serviço DNS. Isso ocorre porque os resolvedores de DNS na Internet costumam solicitar os servidores de nome apenas uma vez a cada dois dias e armazenam a resposta em cache.

Os resolvedores de DNS ainda estão usando as configurações antigas do registro

Se você alterou as configurações em um registro, mas seu tráfego ainda está sendo roteado para o recurso antigo, tal como um servidor web do seu site, uma possível causa é que o DNS ainda tem as configurações anteriores armazenadas em cache. Cada registro tem um valor de TTL (tempo de vida) que especifica por quanto tempo, em segundos, você deseja que os resolvedores de DNS armazenem em cache as informações do registro, como o endereço IP de um servidor web. Até que o total de tempo especificado pelo TTL passe, os resolvedores de DNS continuarão a retornar o valor antigo em resposta às consultas de DNS. Se você quiser saber qual é o TTL de um registro, execute o procedimento a seguir.

> **Note**
>
> Para registros de alias, o TTL é determinado pelo AWS recurso para o qual o registro direciona o tráfego. Para ter mais informações, consulte Escolher entre registros de alias e não alias.

Para exibir o TTL para um registro

1. Faça login AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.
2. Na página Zonas hospedadas, escolha o nome da zona hospedada que inclui o registro.
3. Na lista de registros, encontre o registro cujo valor do TTL você deseja saber e verifique o valor da coluna TTL.

> **Note**
>
> Alterar o TTL agora não fará com que sua alteração tenha efeito mais rapidamente. Os resolvedores de DNS já têm o valor armazenado em cache e eles não receberão a nova configuração até que o tempo especificado pela configuração antiga passe.

Você tem mais de uma zona hospedada com o mesmo nome e atualizou a que não está associada ao domínio

É possível criar mais de uma zona hospedada com o mesmo nome, usando a mesma conta ou usando várias contas. Para especificar a zona hospedada que o Route 53 usa para encaminhar tráfego da Internet para o domínio, obtenha os quatro servidores de nome do Route 53 para essa zona hospedada e atualize o registro de domínio para usar esses servidores de nome.

Se você adicionar, alterar ou excluir registros em uma zona hospedada, mas o registro de domínio estiver usando os servidores de nome de outra zona hospedada, as respostas do Route 53 às consultas de DNS não refletirão as alterações. Para determinar se o registro de domínio está usando os servidores de nome para a zona hospedada na qual você atualizou registros, execute as seguintes tarefas:

1. Determine quais servidores de nomes estão associados ao registro de domínio. Consulte Adicionar ou alterar servidores de nome ou registros cola.
2. Compare os servidores de nomes obtidos na etapa 1 com os servidores de nome que o Route 53 atribuiu à zona hospedada na qual você atualizou os registros. Consulte Obter os servidores de nome de uma zona hospedada pública.

Se os servidores de nome do registro de domínio não corresponderem aos servidores de nome da zona hospedada na qual você atualizou registros, há duas opções:

Altere registros na zona hospedada que está atualmente associada ao domínio (recomendado)

Anote as alterações feitas na zona hospedada que não está associada ao registo de domínio no momento. Depois, acesse a zona hospedada associada ao registro de domínio e faça as mesmas alterações. Esse é o método preferido porque as alterações entram em vigor quase que imediatamente. Para ter mais informações, consulte Editar registros.

Atualize o registro de domínio para usar diferentes servidores de nomes

Altere o registro de domínio para usar os servidores de nome na zona hospedada que você atualizou.

> **Important**
>
> Se você alterar os servidores de nomes associados ao registro de domínio, o domínio ficará indisponível na Internet por até dois dias. Isso ocorre porque os resolvedores DNS

normalmente armazenam em cache os nomes dos servidores de nomes por dois dias. Para obter uma visão geral de como o DNS funciona, incluindo informações sobre o cache do resolvedor, consulte Como o Amazon Route 53 encaminha tráfego para o seu domínio.

Ao alterar os servidores de nomes associados ao registro de domínio, você está essencialmente alterando o serviço de DNS do domínio. Você tem duas opções, dependendo se o domínio está em uso no momento:

- Se o domínio estiver em uso, consulte Tornar o Route 53 o serviço de DNS para um domínio que está em uso.
- Se o domínio estiver inativo no momento, execute as seguintes tarefas:
  1. Obtenha os servidores de nomes da zona hospedada que você deseja usar para rotear o tráfego ao domínio. Consulte Obter os servidores de nome de uma zona hospedada pública.
  2. Na zona hospedada para a qual você obteve servidores de nome na etapa 1, verifique se o registro NS está usando os mesmos quatro servidores de nome. Caso contrário, atualize o registro NS. Consulte Editar registros.
  3. Atualize o registro de domínio para usar os servidores de nome obtidos na etapa 1. Consulte Adicionar ou alterar servidores de nome ou registros cola.

Meu navegador exibe um erro "Servidor não encontrado"

Se o seu navegador exibe um erro "Servidor não encontrado" quando você tenta navegar para um domínio (exemplo.com) ou um subdomínio (www.exemplo.com), aqui estão algumas explicações comuns.

Tópicos

Você não criou um registro para o nome de domínio ou subdomínio

Se você não criar um registro para o domínio ou subdomínio, o DNS não saberá para onde rotear o tráfego quando alguém inserir esse nome em um navegador. Para ter mais informações, consulte Trabalhar com registros.

Você criou um registro, mas especificou o valor incorreto

Quando você cria um registro, é fácil especificar o valor errado, como o endereço IP de um servidor web ou o nome de domínio CloudFront atribuído à sua distribuição na web. Se o registro existe, mas você ainda está recebendo um erro "Servidor não encontrado", recomendamos que confirme se o valor está correto.

O recurso para o qual você está roteando o tráfego está indisponível

Se um registro especifica um recurso como um servidor web que está indisponível, um navegador retornará um erro "Servidor não encontrado". Recomendamos que você verifique o status do recurso para o qual o tráfego está sendo roteado.

Não posso rotear o tráfego para um bucket do Amazon S3 que está configurado para hospedagem de site

Quando você configura um bucket do Amazon S3 para hospedagem de site, é preciso dar ao bucket o mesmo nome que o registro que você deseja usar para encaminhar o tráfego para o bucket. Por exemplo, se você deseja rotear o tráfego de exemplo.com para um bucket do S3 configurado para hospedagem de site, o nome do bucket deve ser exemplo.com.

Se você quiser rotear o tráfego para um bucket do S3 configurado para hospedagem de sites, mas o nome do bucket não aparecer na lista de alvos do console do Amazon Route 53, ou se estiver tentando criar um registro de alias programaticamente e estiver recebendo um InvalidInput erro na API do Route 53, em um dos AWS SDKs, ou, verifique o AWS CLI seguinte: AWS Tools for Windows PowerShell

- O nome do bucket corresponde exatamente ao nome do registro, como exemplo.com ou www.exemplo.com.
- O bucket do S3 está configurado corretamente para hospedagem de site. Para obter mais informações, consulte o tópico sobre como Hospedar um site estático no Amazon S3, no Guia do Usuário do Amazon Simple Storage Service.

Fui cobrado duas vezes pela mesma zona hospedada

Você não será cobrado se excluir uma zona hospedada em até 12 horas depois de ela ter sido criada. Depois de 12 horas, cobramos imediatamente a taxa mensal padrão para uma zona hospedada. A taxa mensal por uma zona hospedada não é dividida proporcionalmente para meses parciais. (A mesma taxa se aplica à zona hospedada que criamos automaticamente quando você registra um domínio.)

Se você criar uma zona hospedada no último dia do mês (por exemplo, 31 de janeiro), a taxa de janeiro pode aparecer na fatura de fevereiro, com a taxa de fevereiro. Observe que o Amazon Route 53 usa o Tempo Universal Coordenado (UTC) como o fuso horário para determinar quando uma zona hospedada foi criada.

Fui cobrado em várias faturas do meu domínio

Quando você se inscreve para uma assinatura, paga uma taxa de registro, uma taxa de transferência ou uma taxa de renovação com um custo inicial, uma fatura exclusiva é gerada. Essa fatura permanece no console de faturamento, mesmo que a transação de pagamento não seja bem-sucedida. O item da linha de cobrança relacionado é mostrado como [x] Quantidade na subseção Registrar-Global da guia Detalhes da fatura por serviço no console de cobrança.

Para visualizar as faturas dispensadas, conclua as seguintes etapas:

Para ver as faturas dispensadas no console de faturamento

1. Faça login no AWS Management Console e abra o AWS Billing console em https://console.aws.amazon.com/billing/.
2. No painel de navegação, selecione Contas.
3. Escolha Faturas para ver os detalhes de todas as faturas dispensadas.

Para ver os pagamentos e reembolsos bem-sucedidos no console de faturamento, conclua as seguintes etapas:

Para confirmar os pagamentos ou reembolsos que foram processados com sucesso

1. No painel de navegação, escolha Payments (Pagamentos).
2. Escolha a guia Transações para ver a tabela Transações de todas as transações concluídas com AWS.

Minha AWS conta foi fechada, suspensa ou encerrada, e meu domínio está registrado no Route 53

Se você encerrou sua AWS conta, ou se a conta for suspensa ou encerrada e a renovação automática estiver ativada, o Route 53 tentará renovar o registro do domínio, mas as renovações falharão. Você pode entrar em contato com o AWS Support e pedir ajuda com as seguintes opções:

- Se você não quiser manter o registro do domínio, o AWS Support pode desativar a renovação automática do domínio. Isso impede que você receba vários e-mails de lembrete sobre a renovação do domínio.
- Se você quiser manter o registro do domínio, o AWS Support pode ajudá-lo a reativar sua conta ou transferir o domínio para outro registrador de domínio.

> **Note**
>
> Depois de 90 dias após o encerramento da sua conta, você não poderá mais reabri-la. Para obter mais informações, consulte Posso reabrir meu arquivo fechado Conta da AWS? .

Para ter mais informações, consulte Entrar em contato com o AWS Support sobre problemas de registro de domínio.

Intervalos de endereço IP dos servidores do Amazon Route 53

A Amazon Web Services (AWS) publica seus intervalos de endereços IP atuais em formato JSON. Se os firewalls ou grupos de segurança restringirem o tráfego de entrada com base em endereços IP de origem, confirme se a sua configuração permite tráfego dos intervalos aplicáveis de endereços IP.

Para visualizar os intervalos atuais de endereços IP para o Route 53, faça download do ip-ranges.json e pesquise o arquivo para obter os seguintes valores:

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

Para obter mais informações sobre endereços IP para AWS recursos, consulte Intervalos de endereços AWS IP no Referência geral da Amazon Web Services.

Intervalos de endereço IP dos servidores de nomes do Route 53

`"service": "ROUTE53"`: esses intervalos de endereços IP são usados por servidores de nomes do Route 53. Adicione esses intervalos à lista de intervalos de endereços IP permitidos se você estiver usando o Route 53 como o serviço de DNS para um ou mais domínios e quiser usar os comandos `dig` ou `nslookup` para consultar servidores de nomes do Route 53.

> **Note**
>
> Raramente alteramos os endereços IP de servidores de nome; se precisarmos alterar endereços IP, você será notificado com antecedência.

Intervalos de endereços IP das verificações de integridade do Route 53

`"service": "ROUTE53_HEALTHCHECKS"`: esses intervalos de endereços IP são usados por verificadores de integridade do Route 53. Adicione esses intervalos à lista de intervalos de endereços

IP permitidos se você estiver usando verificações de integridade do Route 53 para verificar a integridade dos recursos em sua rede.

> **Note**
>
> Raramente alteramos os intervalos de endereços IP dos verificadores de saúde; se precisarmos alterar os intervalos de endereços IP, notificaremos você com antecedência.

Para obter mais informações sobre endereços IP para verificações de integridade, consulte Como configurar regras de roteador e firewall para as verificações de integridade do Amazon Route 53 .

Referenciar listas de prefixos

Uma lista de prefixos é um conjunto de uma ou mais entradas do bloco CIDR que você pode usar para configurar grupos de segurança. O roteador e o firewall para regras da instância do Amazon EC2 devem permitir tráfego oriundo dos endereços IP usados pelos verificadores de integridade do Route 53. Uma referência a uma lista de prefixos ajuda a simplificar o gerenciamento dos blocos CIDR nas regras. Por exemplo, se você especificar frequentemente os mesmos CIDRs de destino em várias tabelas de rotas de gateway de trânsito, poderá gerenciar esses CIDRs em uma única lista de prefixos, em vez de referenciar os mesmos CIDRs diversas vezes em cada tabela de rotas. Se você precisar remover um bloco CIDR, poderá remover a entrada da lista de prefixos em vez de remover a rota de cada regra afetada. Para obter mais informações sobre listas de prefixos em geral, consulte Agrupar blocos CIDR usando listas de prefixos gerenciadas no Manual do usuário da Amazon VPC.

AWS-listas de prefixos gerenciadas são conjuntos de intervalos de endereços IP para AWS serviços. AWS- as listas de prefixos gerenciadas são criadas e mantidas por AWS e podem ser usadas por qualquer pessoa com uma AWS conta. Você não pode criar, modificar, compartilhar ou excluir uma lista AWS de prefixos gerenciada.

Para obter mais informações sobre listas AWS de prefixos gerenciadas, consulte Trabalhar com listas de prefixos AWS gerenciadas no Guia do usuário da Amazon VPC.

Intervalos de endereços IP das verificações de integridade do Route 53

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`: o Route 53 só usa esses intervalos de endereços IP internamente. Não é necessário adicionar esses intervalos à lista de intervalos permitidos.

Marcação de recursos do Amazon Route 53

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor, ambos definidos por você. Por exemplo, a chave pode ser "domínio" e o valor pode ser "exemplo.com". Você pode usar tags para uma variedade de propósitos; um uso comum é a categorização e o rastreamento dos custos do Amazon Route 53. Quando você aplica tags a zonas hospedadas, domínios e verificações de integridade do Route 53, a AWS gera um relatório de alocação de custos como um arquivo CSV (valor separado por vírgulas), cujo uso e custos são agregados por tags. É possível aplicar tags que representem categorias de negócios (como centros de custos, nomes de aplicações ou proprietários) para organizar seus custos de vários serviços. Para obter mais informações sobre como usar tags para alocação de custos, consulte Como usar tags de alocação de custo no Manual do usuário do AWS Billing.

Para facilidade de uso e melhores resultados, use o Tag Editor no AWS Management Console, que fornece uma forma unificada e central para criar e gerenciar suas tags. Para obter mais informações, consulte Como trabalhar com o Tag Editor em Conceitos básicos do AWS Management Console. Você também pode usar o console do Route 53 para aplicar tags para alguns recursos:

- Health checks (Verificações de integridade): para obter mais informações, consulte Nomear e adicionar tags às verificações de integridade.
- Route 53 Resolver inbound endpoints (Endpoints de entrada do Route 53 Resolver): para obter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada.
- Resolver outbound endpoints (Endpoints de saída do Resolver): para obter mais informações, consulte Valores especificados ao criar ou editar endpoints de saída.
- Resolver rules (Regras do Resolver): para obter mais informações, consulte Valores especificados ao criar ou editar regras.
- Zonas hospedadas: para obter mais informações, consulte Trabalhar com zonas hospedadas.

> **Note**
>
> As cobranças do Resolver se baseiam em parte nas interfaces de rede elástica da VPC, que correspondem aos endereços IP especificados para endpoints de entrada e de saída. No momento, você não pode marcar interfaces de rede elástica criadas pelo Resolver, portanto, você não pode usar tags para alocar custos para o Resolver. Para obter mais informações sobre preço do Resolver, consulte Preço do Amazon Route 53.

Você também pode aplicar tags aos recursos usando a API do Route 53. Para obter mais informações, consulte as ações relacionadas a tags no tópico Ações da API do Route 53 por função na Referência da API do Amazon Route 53.

Tutoriais

Os seguintes tutoriais explicam como usar o Amazon Route 53 como o serviço DNS para um subdomínio junto com outro serviço DNS para o domínio e como usar o Route 53 para vários casos de uso relacionados a registros ponderados e de latência.

Tópicos

Como usar o Amazon Route 53 como o serviço DNS dos subdomínios sem migrar o domínio pai

Você pode usar o Amazon Route 53 como o serviço DNS de um subdomínio novo ou existente e ainda usar outro serviço DNS para o domínio pai. Para obter mais informações, consulte o tópico aplicável.

Tópicos

Criação de um subdomínio que usa o Amazon Route 53 como serviço DNS, sem migrar o domínio pai

Você pode criar um subdomínio que usa o Amazon Route 53 como serviço DNS, sem migrar o domínio pai de outro serviço DNS.

O processo tem as seguintes etapas básicas:

1. Verifique se você deve usar este procedimento.
2. Crie uma zona hospedada do Route 53 para o subdomínio.
3. Adicione registros do novo subdomínio à sua zona hospedada do Route 53.
4. API only (Somente API): confirme se as alterações foram propagadas para todos os servidores DNS do Route 53.

> **Note**
>
> Atualmente, a única maneira de verificar se as alterações foram propagadas é usar a ação da API GetChange. Geralmente, as alterações são propagadas para todos os servidores de nome do Route 53 dentro de 60 segundos.

5. Atualizar o serviço de DNS do domínio pai ao adicionando registros de servidor de nome ao subdomínio.

Determinação de quais procedimentos usar para a criação de um subdomínio

Os procedimentos deste tópico explicam como executar uma operação incomum. Se você já estiver usando o Route 53 como serviço DNS para seu domínio e quiser apenas encaminhar o tráfego de um subdomínio, como www.exemplo.com, para seus recursos, como um servidor Web em execução em uma instância do EC2, consulte Rotear tráfego para subdomínios.

Use esse procedimento somente se estiver usando outro serviço DNS para um domínio, como example.com, e deseja começar a usar o Route 53 como o serviço DNS de um novo subdomínio desse domínio, como www.example.com.

Criar uma zona hospedada para o novo subdomínio

Quando você quiser usar o Amazon Route 53 como o serviço DNS para um novo subdomínio sem migrar o domínio pai, comece criando uma zona hospedada para o subdomínio. O Route 53 armazena informações sobre seu subdomínio na zona hospedada.

Para obter informações sobre como criar uma zona hospedada usando o console do Route 53, consulte Criar uma zona hospedada pública.

Criar registros

Você pode criar registros usando o console do Amazon Route 53 ou a API do Route 53. Os registros que você cria no Route 53 se tornarão os registros que o DNS usará depois que você delegar a

responsabilidade do subdomínio ao Route 53, conforme explicado em Atualizar o serviço de DNS com registros de servidor de nome do subdomínio, posteriormente no processo.

> **Important**
>
> Não crie registros adicionais de servidor de nome (NS) ou de início de autoridade (SOA) na zona hospedada do Route 53. Não exclua os registros de NS e SOA existentes.

Para criar registros usando o console do Route 53, consulte Trabalhar com registros. Para criar registros usando a API do Route 53, use `ChangeResourceRecordSets`. Para obter mais informações, consulte ChangeResourceRecordSets na Referência da API do Amazon Route 53.

Verificar o status das suas alterações (somente na API)

A criação de uma nova zona hospedada e a alteração de registros levam tempo para se propagar para os servidores DNS do Route 53. Se você usou ChangeResourceRecordSets para criar seus registros, pode usar a ação `GetChange` para determinar se suas alterações foram propagadas. (`ChangeResourceRecordSets` retorna um valor para `ChangeId`, que você pode incluir em uma solicitação `GetChange` subsequente. `ChangeId` não estará disponível se você tiver criado os registros usando o console.) Para obter mais informações, consulte GET GetChange na Referência da API do Amazon Route 53.

> **Note**
>
> Geralmente, as alterações são propagadas para todos os servidores de nome do Route 53 dentro de 60 segundos.

Atualizar o serviço de DNS com registros de servidor de nome do subdomínio

Depois que as alterações nos registros do Amazon Route 53 tiverem sido propagadas (consulte Verificar o status das suas alterações (somente na API)), atualize o serviço DNS do domínio pai adicionando registros de NS ao subdomínio. Esse processo é conhecido como delegação de responsabilidade do subdomínio para o Route 53. Por exemplo, se o domínio pai example.com estiver hospedado com outro serviço DNS e você tiver criado o subdomínio test.example.com no Route 53, atualize o serviço DNS para example.com com novos registros de NS para test.example.com.

Execute o procedimento a seguir.

1. Usando o método fornecido pelo serviço de DNS, faça backup do arquivo de zona do domínio pai.
2. No console do Route 53, obtenha os servidores de nome para sua zona hospedada do Route 53:

   a. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   b. No painel de navegação, clique em Hosted zones (Zonas hospedadas).

   c. Na página Hosted zones (Zonas hospedadas), escolha o botão de opção (não o nome) da zona hospedada, depois escolha View details (Exibir detalhes).

   d. Na página de detalhes da zona hospedada, escolha Hosted zone details (Detalhes da zona hospedada).

   e. Anote os quatro servidores listados para Name servers (Servidores de nome).

   Você também pode usar a ação `GetHostedZone`. Para obter mais informações, consulte GetHostedZone na Referência da API do Amazon Route 53.
3. Usando o método fornecido pelo serviço de DNS do domínio pai, adicione registros de NS do subdomínio ao arquivo de zona do domínio pai. Nesses registros de NS, especifique os quatro servidores do Route 53 associados à zona hospedada que você criou na etapa 1.

> **Important**
>
> Não adicione um registro de início de autoridade (SOA) ao arquivo de zona para o domínio pai. Como o subdomínio usará o Route 53, o serviço de DNS do domínio pai não será a autoridade para o subdomínio.
>
> Se o serviço de DNS adicionou automaticamente um registro de SOA ao subdomínio, exclua o registro do subdomínio. No entanto, não exclua o registro de SOA do domínio pai.

Migrar o serviço DNS de um subdomínio para o Amazon Route 53 sem migrar o domínio pai

Você pode migrar um subdomínio para usar o Amazon Route 53 como serviço DNS sem migrar o domínio pai de outro serviço DNS.

O processo tem as seguintes etapas básicas:

1. Verifique se você deve usar este procedimento.
2. Crie uma zona hospedada do Route 53 para o subdomínio.
3. Obtenha a configuração de DNS atual do provedor de serviço de DNS atual para o domínio pai.
4. Adicione registros do subdomínio à sua zona hospedada do Route 53.
5. API only (Somente API): confirme se as alterações foram propagadas para todos os servidores DNS do Route 53.

   > **Note**
   >
   > Atualmente, a única maneira de verificar se as alterações foram propagadas é usar a ação da API GetChange. Geralmente, as alterações são propagadas para todos os servidores de nome do Route 53 dentro de 60 segundos.

6. Atualize a configuração de DNS com o provedor de serviço de DNS para o domínio pai adicionando registros de servidor de nome ao subdomínio.

Determinação de quais procedimentos usar para a criação de um subdomínio

Os procedimentos deste tópico explicam como executar uma operação incomum. Se você já estiver usando o Route 53 como serviço DNS para seu domínio e quiser apenas encaminhar o tráfego de um subdomínio, como www.exemplo.com, para seus recursos, como um servidor Web em execução em uma instância do EC2, consulte Rotear tráfego para subdomínios.

Use esse procedimento somente se estiver usando outro serviço DNS para um domínio, como example.com, e deseja começar a usar o Route 53 como o serviço DNS de um subdomínio existente desse domínio, como www.example.com.

Criar uma zona hospedada para o subdomínio

Se você quiser migrar um subdomínio de outro serviço DNS para o Amazon Route 53, mas não quiser migrar o domínio pai, comece criando uma zona hospedada para o subdomínio. O Route 53 armazena informações sobre seu subdomínio na zona hospedada.

Para obter informações sobre como criar uma zona hospedada usando o console do Route 53, consulte Criar uma zona hospedada pública.

Obter a configuração de DNS atual do provedor de serviço de DNS

Para simplificar o processo de migração de um subdomínio existente para o Route 53, obtenha a configuração de DNS atual do domínio do provedor de serviço DNS que está servindo o domínio no momento. Você pode usar essas informações como base para a configurar o Route 53 como o serviço DNS para o subdomínio.

As informações solicitadas bem como seu formato dependem da empresa que você está usando como provedor de serviço de DNS. Idealmente, eles fornecerão um arquivo de zona, que contém informações sobre todos os registros na sua configuração atual. (Os registros informam ao DNS como você deseja que o tráfego seja encaminhado para seus domínios e subdomínios. Por exemplo, quando alguém informa o nome de seu domínio em um navegador da Web, você deseja que o tráfego seja encaminhado para um servidor Web em seu datacenter, para uma instância do Amazon EC2, para uma distribuição do CloudFront ou para algum outro local?) Se você conseguir obter um arquivo de zona do seu provedor de serviços DNS atual, poderá editar esse arquivo para remover os registros que não deseja migrar para o Amazon Route 53. Em seguida, você pode importar os demais registros para sua zona hospedada do Route 53, o que simplifica bastante o processo. Entre em contato com o atendimento ao cliente do provedor de serviço de DNS atual para obter um arquivo de zona ou uma lista de registros.

Criar registros

Usando os registros obtidos do provedor de serviços DNS atual, como um ponto de partida, crie registros correspondentes na zona hospedada do Amazon Route 53 que você criou para o subdomínio. Os registros que você cria no Route 53 se tornarão os registros que o DNS usará depois que você delegar a responsabilidade do subdomínio ao Route 53, conforme explicado em Atualizar o serviço de DNS com registros de servidor de nome do subdomínio, posteriormente no processo.

> **Important**
>
> Não crie registros adicionais de servidor de nome (NS) ou de início de autoridade (SOA) na zona hospedada do Route 53. Não exclua os registros de NS e SOA existentes.

Para criar registros usando o console do Route 53, consulte Trabalhar com registros. Para criar registros usando a API do Route 53, use `ChangeResourceRecordSets`. Para obter mais informações, consulte ChangeResourceRecordSets na Referência da API do Amazon Route 53.

Verificar o status das suas alterações (somente na API)

A criação de uma nova zona hospedada e a alteração de registros levam tempo para se propagar para os servidores DNS do Route 53. Se você usou ChangeResourceRecordSets para criar seus registros, pode usar a ação `GetChange` para determinar se suas alterações foram propagadas. (`ChangeResourceRecordSets` retorna um valor para `ChangeId`, que você pode incluir em uma solicitação `GetChange` subsequente. `ChangeId` não estará disponível se você tiver criado os registros usando o console.) Para obter mais informações, consulte GET GetChange na Referência da API do Amazon Route 53.

> **Note**
>
> Geralmente, as alterações são propagadas para todos os servidores de nome do Route 53 dentro de 60 segundos.

Atualizar o serviço de DNS com registros de servidor de nome do subdomínio

Depois que as alterações nos registros do Amazon Route 53 tiverem sido propagadas (consulte Verificar o status das suas alterações (somente na API)), atualize o serviço DNS do domínio pai adicionando registros de NS ao subdomínio. Esse processo é conhecido como delegação de responsabilidade do subdomínio para o Route 53. Por exemplo, suponha que o domínio pai example.com esteja hospedado com outro serviço DNS e que você esteja migrando o subdomínio test.example.com para o Route 53. Você deve criar uma zona hospedada para test.example.com e atualizar o serviço de DNS para example.com com os registros de NS que o Route 53 atribuiu à nova zona hospedada para test.example.com.

Execute o procedimento a seguir.

1. Usando o método fornecido pelo serviço de DNS, faça backup do arquivo de zona do domínio pai.
2. Se o provedor de serviços de DNS anterior do domínio tem um método para alterar as configurações de TTL para seus servidores de nome, recomendamos que você altere as configurações para 900 segundos. Isso limita o tempo durante o qual as solicitações de clientes tentarão resolver nomes de domínio usando servidores de nome obsoletos. Se o TTL atual é 172.800 segundos (dois dias), que é uma configuração padrão, você ainda precisa aguardar dois dias para que resolvedores e clientes interrompam o armazenamento em cache de registros de DNS usando o TTL anterior. Depois que as configurações de TTL expirarem, você poderá excluir com segurança os registros armazenados no provedor anterior e fazer alterações apenas no Route 53.
3. No console do Route 53, obtenha os servidores de nome para sua zona hospedada do Route 53:

   a. Faça login no AWS Management Console e abra o console do Route 53 em https://console.aws.amazon.com/route53/.

   b. No painel de navegação, clique em Hosted zones (Zonas hospedadas).

   c. Na página Hosted zones (Zonas hospedadas), escolha o botão de opção (não o nome) da zona hospedada, depois escolha View details (Exibir detalhes).

   d. Na página de detalhes da zona hospedada, escolha Hosted zone details (Detalhes da zona hospedada).

   e. Anote os quatro servidores listados para Name servers (Servidores de nome).

   Você também pode usar a ação `GetHostedZone`. Para obter mais informações, consulte GetHostedZone na Referência da API do Amazon Route 53.
4. Usando o método fornecido pelo serviço de DNS do domínio pai, adicione registros de NS do subdomínio ao arquivo de zona do domínio pai. Dê aos registros de NS o mesmo nome do subdomínio. Para os valores nos registros de NS, especifique os quatro servidores de nome do Route 53 associados à zona hospedada que você criou na etapa 2. Observe que diferentes serviços de DNS usam terminologia diferente. Talvez você precise entrar em contato com o suporte técnico do seu serviço de DNS para saber como executar esta etapa.

> **Important**
>
> Não adicione um registro de início de autoridade (SOA) ao arquivo de zona para o domínio pai. Como o subdomínio usará o Route 53, o serviço de DNS do domínio pai não será a autoridade para o subdomínio.
> Se o serviço de DNS adicionou automaticamente um registro de SOA ao subdomínio, exclua o registro do subdomínio. No entanto, não exclua o registro de SOA do domínio pai.

Dependendo das configurações de TTL dos servidores de nome do domínio pai, a propagação das alterações para os resolvedores de DNS pode levar 48 horas ou mais. Durante esse período, os resolvedores de DNS ainda podem responder a solicitações com os servidores de nome para o serviço de DNS do domínio pai. Além disso, os computadores cliente podem continuar a ter servidores de nome anterior para o subdomínio no cache.

5. Depois que as configurações de TTL do registrador do domínio expirarem (consulte a etapa 2), exclua os seguintes registros do arquivo de zona para o domínio pai:

   - Os registros que você adicionou ao Route 53, conforme descrito em Criar registros.
   - Seus registros de NS do serviço de DNS. Ao concluir a exclusão de registros de NS, os únicos registros de NS no arquivo de zona serão os criados na etapa 4.

Passar para o encaminhamento por latência no Amazon Route 53

Com o encaminhamento por latência, o Amazon Route 53 pode direcionar seus usuários para o endpoint de mais baixa latência disponível da AWS. Por exemplo, você pode associar um nome DNS como `www.example.com` a um ELB Classic, uma Aplicação ou um Network Load Balancer ou a instâncias do Amazon EC2 ou endereços de IP elásticos que são hospedados nas regiões Leste dos EUA (Ohio) e Europa (Irlanda). O servidores DNS do Route 53 decidem, de acordo com as condições de rede das duas semanas anteriores, quais instâncias em quais regiões devem atender a usuários específicos. Um usuário em Londres provavelmente será direcionado para a instância da Europa (Irlanda), um usuário em Chicago provavelmente será direcionado para a instância do Leste dos EUA (Ohio) e assim por diante. O Route 53 oferece suporte ao encaminhamento por latência para os registros A, AAAA, TXT e CNAME, bem como aliases para registros A e AAAA.

> **Note**
>
> Os dados sobre a latência entre usuários e seus recursos são baseados totalmente no tráfego entre usuários e datacenters da AWS. Se você não estiver usando recursos em uma região da AWS, a latência real entre seus usuários e recursos poderá variar significativamente em relação aos dados de latência da AWS. Isso ocorrerá mesmo se seus recursos estiverem localizados na mesma cidade que uma região da AWS.

Para obter uma transição tranquila e de baixo risco, você pode combinar registros de latência e ponderados para migrar gradualmente do roteamento padrão para o roteamento baseado em latência com controle total e o recurso de reversão em cada estágio. Vamos considerar um exemplo em que `www.example.com` está hospedado em uma instância do Amazon EC2 na região Leste dos EUA (Ohio). A instância tem o endereço IP elástico `W.W.W.W`. Suponha que você queira continuar roteando o tráfego para a região Leste dos EUA (Ohio) quando aplicável, enquanto também começa a direcionar usuários para as instâncias adicionais do Amazon EC2 na região Oeste dos EUA (Norte da Califórnia) (IP elástico `X.X.X.X`) e na região Europa (Irlanda) (IP elástico `Y.Y.Y.Y`). A zona hospedada do Route 53 de `example.com` já tem um registro para `www.example.com` que tem um Type (Tipo) A e um Value (Valor) (um endereço IP) de `W.W.W.W`.

Quando você concluir o exemplo a seguir, terá dois registros de alias ponderados:

- Você converterá os registros existentes para `www.example.com` em um registro de alias ponderado que continua a direcionar a maior parte do tráfego para a instância do Amazon EC2 existente na região Leste dos EUA (Ohio).
- Você criará outro registro de alias ponderado que inicialmente direciona apenas uma pequena parte do tráfego para seus registros de latência, o que roteia o tráfego para todas as três regiões.

Ao atualizar os pesos nesses registros de alias ponderados, você pode mudar gradualmente do roteamento do tráfego apenas para a região Leste dos EUA (Ohio) para roteamento do tráfego para todas as três regiões nas quais você tem instâncias do Amazon EC2.

Como passar para o roteamento baseado em latência

1. Faça uma cópia do registro de `www.example.com`, mas use um novo nome de domínio, por exemplo, `copy-www.example.com`. Dê ao novo registro o mesmo Tipo (A) e Valor (`W.W.W.W`) como o registro de `www.example.com`.

2. Atualize o registro A existente para `www.example.com` a fim de torná-lo um registro de alias ponderado:

   - Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to another record in this hosted zone (Alias para outro registro nessa zona hospedada), e especifique `copy-www.example.com`.
   - Para Weight (Peso), especifique 100.

   Ao concluir a atualização, o Route 53 continuará a usar esse registro para encaminhar todo o tráfego para o recurso que tenha um endereço IP de `W.W.W.W`.
3. Crie um registro de latência para cada uma de suas instâncias do Amazon EC2, por exemplo:

   - Leste dos EUA (Ohio), endereço de IP elástico `W.W.W.W`
   - Oeste dos EUA (Norte da Califórnia), endereço de IP elástico `X.X.X.X`
   - Europa (Irlanda), endereço de IP elástico `Y.Y.Y.Y`

   Dê a todos os registros de latência o mesmo nome de domínio, por exemplo, `www-lbr.example.com` e o mesmo tipo A.

   Quando você terminar de criar os registros de latência, o Route 53 continuará roteando o tráfego usando o registro que você atualizou na etapa 2.

   Você pode usar `www-lbr.example.com` para testes de validação, por exemplo, a fim de garantir que cada endpoint pode aceitar solicitações.
4. Agora vamos adicionar o registro de latência `www-lbr.example.com` ao registro ponderado `www.example.com` e começar o roteamento limitado do tráfego para as instâncias correspondentes do Amazon EC2. Isso significa que a instância do Amazon EC2 na região Leste dos EUA (Ohio) obterá o tráfego dos dois registros ponderados.

   Crie outro registro de alias ponderado para `www.example.com`:

   - Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to another record in this hosted zone (Alias para outro registro nessa zona hospedada), e especifique `www-lbr.example.com.`
   - Para Weight (Peso), especifique 1.

Quando você terminar e suas alterações estiverem sincronizadas com os servidores do Route 53, o Route 53 começará a encaminhar uma pequena fração de seu tráfego (1/101) para as instâncias do Amazon EC2 para as quais você criou registros de latência na etapa 3.

5. À medida que você desenvolver a confiança de que os endpoints estão adequadamente dimensionados para o tráfego de entrada, ajuste os pesos. Por exemplo, se você quer que 10% de suas solicitações sejam fundamentadas no roteamento baseado em latência, altere os pesos para 90 e 10, respectivamente.

Para obter mais informações sobre como criar registros de latência, consulte Criar registros usando o console do Amazon Route 53.

Como adicionar outra região ao encaminhamento por latência no Amazon Route 53

Se você estiver usando o roteamento baseado em latência e quiser adicionar uma instância a uma nova região, poderá migrar o tráfego gradualmente para a nova região da mesma forma que alterou o tráfego para o roteamento baseado em latência Passar para o encaminhamento por latência no Amazon Route 53.

Por exemplo, suponha que você esteja usando o encaminhamento por latência para encaminhar o tráfego para `www.example.com`, e queira adicionar uma instância do Amazon EC2 na Ásia-Pacífico (Tóquio) para suas instâncias no Leste dos EUA (Ohio), Oeste dos EUA (Norte da Califórnia) e Europa (Irlanda). O procedimento de exemplo a seguir explica uma forma de adicionar uma instância em outra região.

Neste exemplo, a zona hospedada do Amazon Route 53 para `example.com` já tem um registro de alias ponderado para `www.example.com` que está roteando o tráfego para os registros com base em latência para `www-lbr.example.com`:

- Leste dos EUA (Ohio), endereço de IP elástico `W.W.W.W`
- Oeste dos EUA (Norte da Califórnia), endereço de IP elástico `X.X.X.X`
- Europa (Irlanda), endereço de IP elástico `Y.Y.Y.Y`

O registro de alias ponderado tem um peso 100. Após a transição para o roteamento baseado em latência, suponha que você tenha excluído o outro registro ponderado usado para a transição.

Como adicionar outra região ao encaminhamento por latência no Route 53

1. Crie quatro novos registros de latência que incluem três regiões originais bem como a nova região para a qual você deseja iniciar o roteamento de tráfego.

   - Leste dos EUA (Ohio), endereço de IP elástico `W.W.W.W`
   - Oeste dos EUA (Norte da Califórnia), endereço de IP elástico `X.X.X.X`
   - Europa (Irlanda), endereço de IP elástico `Y.Y.Y.Y`
   - Ásia-Pacífico (Tóquio), Endereço de IP elástico `Z.Z.Z.Z`

   Dê a todos os registros de latência o mesmo novo nome de domínio, por exemplo, `www-lbr-2012-04-30.example.com` e o mesmo tipo A.

   Quando você concluir a criação dos registros de latência, o Route 53 continuará encaminhando o tráfego usando o registro de alias ponderado original (`www.example.com`) e os registros de latência (`www-lbr.example.com`).

   Você pode usar os registros `www-lbr-2012-04-30.example.com` para testes de validação, por exemplo, a fim de garantir que cada endpoint pode aceitar solicitações.
2. Crie um registro de alias ponderado para os novos registros de latência:

   - Para o nome de domínio, especifique o nome do registro de alias ponderado existente, `www.example.com`.
   - Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to another record in this hosted zone (Alias para outro registro nessa zona hospedada), e especifique `www-lbr-2012-04-30.example.com`.
   - Para Weight (Peso), especifique 1.

   Quando você concluir, o Route 53 começará a encaminhar uma pequena fração do tráfego (1/101) para as instâncias do Amazon EC2 para as quais você criou registros de latência de `www-lbr-2012-04-30.example.com` na etapa 1. O restante do tráfego continuará a ser encaminhado para os registros de latência `www-lbr.example.com`, que não incluem a instância do Amazon EC2 na região Ásia-Pacífico (Tóquio).
3. À medida que você desenvolver a confiança de que os endpoints estão adequadamente dimensionados para o tráfego de entrada, ajuste os pesos. Por exemplo, se você quer que 10% de suas solicitações sejam roteadas para registros de latência que incluem a região

de Tóquio, altere o peso de `www-lbr.example.com` de 100 para 90 e o peso de `www-lbr-2012-04-30.example.com` de 1 a 10.

Para obter mais informações sobre a criação de registros, consulte Criar registros usando o console do Amazon Route 53.

Como usar registros de latência e ponderados no Amazon Route 53 para encaminhar tráfego para várias instâncias do Amazon EC2 em uma região

Se sua aplicação estiver em execução em instâncias do Amazon EC2 em duas ou mais regiões do Amazon EC2, e se você tiver mais de uma instância do Amazon EC2 em uma ou mais regiões, você poderá usar o encaminhamento por latência para encaminhar o tráfego para a região correta e, em seguida, usar registros ponderados para encaminhar o tráfego para instâncias dentro da região com base nos pesos especificados.

Por exemplo, suponha que você tenha três instâncias do Amazon EC2 com endereços de IP elásticos na região Leste dos EUA (Ohio) e que você deseja distribuir de maneira uniforme as solicitações entre os três IPs para os usuários para os quais a região Leste dos EUA (Ohio) é apropriada. Apenas uma instância do Amazon EC2 é suficiente em outras regiões, embora você possa aplicar a mesma técnica a muitas regiões de uma só vez.

Para usar registros de latência e ponderados no Amazon Route 53 para encaminhar tráfego para várias instâncias do Amazon EC2 em uma região

1. Crie um grupo de registros ponderados para as instâncias do Amazon EC2 na região. Observe o seguinte:

   - Dê a cada registro ponderado o mesmo valor de Record name (Nome do registro) (por exemplo, `us-east.example.com`) e Record type (Tipo de registro).
   - Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha o endereço IP ou outro valor dependendo do tipo de registro e especifique o valor de um dos endereços de IP elástico.
   - Se você quiser dar o mesmo peso às instâncias do Amazon EC2, especifique o mesmo valor para Weight (Peso).
   - Especifique um valor exclusivo para Definir ID para cada registro.

Para obter mais informações sobre valores de registros ponderados, consulte Roteamento ponderado

2. Se você tiver várias instâncias do Amazon EC2 em outras regiões, repita a etapa 1 para as outras regiões. Especifique um valor diferente para Nome em cada região.
3. Para cada região em que você tem várias instâncias do Amazon EC2 (por exemplo, Leste dos EUA [Ohio]), crie um registro de alias de latência. Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha Alias to another record in this hosted zone (Alias para outro registro nessa zona hospedada) e especifique o valor do campo Record name (Nome do registro) (por exemplo, `us-east.example.com`) que você atribuiu aos registros ponderados nessa região.
4. Para cada região em que você tenha uma instância do Amazon EC2, crie um registro de latência. Para o valor de Record name (Nome do registro), especifique o mesmo valor que você especificou para os registros de alias de latência criados na etapa 3. Para Value/Route traffic to (Valor/Encaminhar tráfego para), escolha o endereço IP ou outro valor dependendo do tipo de registro e especifique o endereço de IP elástico da instância do Amazon EC2 nessa região.

   Para saber mais sobre como adicionar registros de alias a instâncias do Amazon EC2, consulteComo encaminhar o tráfego para uma instância do Amazon EC2

Para obter mais informações sobre a criação de registros, consulte Criar registros usando o console do Amazon Route 53.

Como gerenciar mais de 100 registros ponderados no Amazon Route 53

O Amazon Route 53 permite que você configure registros ponderados. Para um determinado nome e tipo (por exemplo, `www.example.com`, tipo A), você pode configurar até 100 respostas alternativas, cada uma com seu próprio peso. Ao responder às consultas de `www.example.com`, os servidores DNS do Route 53 selecionam uma resposta aleatória ponderada para retornar aos resolvedores de DNS. O valor de um registro ponderado que tem um peso 2 costuma ser retornado duas vezes mais que o valor de um registro ponderado que tem um peso 1.

Se você precisa direcionar o tráfego para mais de 100 endpoints, uma maneira de fazer isso é usar uma árvore de registros de alias ponderados e registros ponderados. Por exemplo, o primeiro “nível” da árvore pode ser de até 100 registros de alias ponderados, sendo que cada um deles pode, por

sua vez, apontar para até 100 registros ponderados. O Route 53 permite até três níveis de recursão, possibilitando que você gerencie até 1.000.000 endpoints exclusivos ponderados.

Um árvore simples dois níveis pode ter a seguinte aparência:

Registros de alias ponderados

- aliases `www.example.com` para `www-a.example.com` com peso 1
- aliases `www.example.com` para `www-b.example.com` com peso 1

Registros ponderados

- `www-a.example.com`, tipo A, valor 192.0.2.1, peso 1
- `www-a.example.com`, tipo A, valor 192.0.2.2, peso 1

- `www-b.example.com`, tipo A, valor 192.0.2.3, peso 1
- `www-b.example.com`, tipo A, valor 192.0.2.4, peso 1

Para obter mais informações sobre a criação de registros, consulte Trabalhar com registros.

Como ponderar respostas de vários registros tolerantes a falha no Amazon Route 53

> **Note**
>
> Os registros que usam a política de roteamento de resposta com valores múltiplos se comportam da mesma maneira que a configuração documentada neste tutorial. A principal diferença é que a configuração do tutorial permite que você especifique pesos, o que pode ser útil quando seus endpoints têm capacidades diferentes. Para obter mais informações, consulte Roteamento de resposta com vários valores.

Um registro ponderado do Amazon Route 53 só pode ser associado a um registro, o que significa uma combinação de um nome (por exemplo, `example.com`) e um tipo de registro (por exemplo, A). Mas em geral é desejável ponderar as respostas de DNS que contêm vários registros.

Por exemplo, você pode ter oito instâncias do Amazon EC2 ou endpoints de IP elástico para um serviço. Se os clientes do serviço oferecem suporte a tentativas de conexão (como fazem todos os navegadores comuns), fornecer vários endereços IP em respostas DNS permitirá que esses clientes tenham endpoints alternativos em caso de falha de qualquer endpoint específico. Você pode até se proteger contra a falha de uma zona de disponibilidade caso configure as respostas para conter uma combinação de IPs hospedados em duas ou mais zonas de disponibilidade.

As respostas de vários registros também são úteis quando um grande número de clientes (por exemplo, aplicativos web móveis) compartilham um pequeno conjunto de caches DNS. Neste caso, as respostas de vários registros permitem que os clientes direcionem solicitações para vários endpoints, mesmo se eles receberem uma resposta DNS comum do cache compartilhado.

Esses tipos de respostas ponderadas de vários registros podem ser obtidos usando uma combinação de registros e registros de alias ponderados. Você pode agrupar oito endpoints em dois conjuntos de registros distintos que contêm quatro endereços IP cada:

`endpoint-a.example.com`, tipo A, com os seguintes valores:

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

`endpoint-b.example.com`, tipo A, com os seguintes valores:

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

Em seguida, você pode criar um registro de alias ponderado que aponta para cada grupo:

- aliases `www.example.com` para `endpoint-a.example.com`, tipo A, peso 1
- aliases `www.example.com` para `endpoint-b.example.com`, tipo A, peso 1

Para obter mais informações sobre a criação de registros, consulte Trabalhar com registros.

Práticas recomendadas do Amazon Route 53

Siga estas práticas recomendadas ao configurar o Route 53.

Tópicos

Práticas recomendadas do Amazon Route 53 DNS

Siga estas práticas recomendadas para obter os melhores resultados ao usar o serviço de DNS do Amazon Route 53.

Usar as funções do plano de dados para failover de DNS e recuperação de aplicações

Os planos de dados do Route 53, inclusive verificações de integridade, e o controle de roteamento do Amazon Route 53 Application Recovery Controller são distribuídos globalmente e foram projetados para fornecer 100% de disponibilidade e funcionalidade, mesmo durante eventos graves. Integram-se entre si e não dependem da funcionalidade do ambiente de gerenciamento. Embora os ambientes de gerenciamento desses serviços, inclusive seus consoles, sejam geralmente muito confiáveis, são projetados de maneira mais centralizada e priorizam durabilidade e consistência em vez de alta disponibilidade. Para cenários como failover durante recuperação de desastres, recomendamos usar recursos como as verificações de integridade do Route 53 e o controle de roteamento do Route 53 ARC que contam com a funcionalidade de plano de dados para atualizar o DNS. Para obter mais informações, consulte Conceitos de planos de dados e de controle e Criar mecanismos de recuperação de desastres usando o Amazon Route 53.

Escolher valores de TTL para registros de DNS

O TTL do DNS é o valor numérico (em segundos) que os resolvedores de DNS usam para decidir por quanto tempo um registro poderá ser armazenado em cache sem fazer outra consulta ao Route 53. Todos os registros de DNS devem ter um TTL especificado. O intervalo recomendado para valores de TTL é de 60 a 172.800 segundos.

A escolha de um TTL envolve um equilíbrio entre latência e confiabilidade e capacidade de resposta à mudança. Com TTLs mais curtos em um registro, os resolvedores de DNS perceberão

atualizações no registro mais rapidamente, pois deverão consultar com mais frequência. Isso aumenta o volume (e o custo) das consultas. Quanto mais se prolonga o TTL, maior é a frequência com que os resolvedores de DNS respondem a consultas do cache, o que geralmente é mais rápido, mais barato e, em algumas situações, mais confiável porque evita consultas na Internet. Não há valor correto, mas vale a pena pensar no que é mais importante para você: capacidade de resposta ou confiabilidade.

Fatos a considerar ao definir valores de TTL:

- Defina TTLs de registro de DNS pelo tempo que você pode esperar para que uma alteração entre em vigor. Isso se aplica principalmente a delegações (conjuntos de registros de NS) ou outros registros que raramente são alterados, como registros MX. Para esses registros, TTLs mais longos são recomendados. É comum escolher um valor entre uma hora (3600 s) e um dia (86.400 s).
- Para registros que precisam ser alterados como parte de um mecanismo de failover rápido (principalmente registros com verificação de integridade), convém usar TTLs mais curtos. Definir um TTL de 60 ou 120 segundos é comum para esse cenário.
- Quando quiser fazer alterações em entradas DNS críticas, recomendamos que você reduza temporariamente os TTLs. Em seguida, faça as alterações, observe e reverta rapidamente, se precisar. Depois que as alterações forem finalizadas e estiverem funcionando conforme o esperado, você poderá aumentar o TTL.

Para mais informações, consulte TTL (segundos).

Registros CNAME

Os registros CNAME ne DNS são uma forma de apontar um nome de domínio para outro. Se um resolvedor de DNS resolver domain-1.example.com e encontrar um CNAME que aponta para domain-2.example.com, o resolvedor de DNS deverá prosseguir para resolver domain-2.example.com antes de responder. Esses registros são úteis em muitas situações, por exemplo, para garantir consistência quando um site tem mais de um nome de domínio.

Porém, os resolvedores de DNS devem fazer mais consultas para responder aos CNAMES, o que aumenta a latência e os custos. Sempre que possível, uma alternativa mais rápida e mais barata é usar um registro de alias do Route 53. Os registros de aliases permitem que o Route 53 responda com uma resposta direta para AWS recursos (por exemplo, um balanceador de carga) e para outros domínios na mesma zona hospedada.

Para ter mais informações, consulte Encaminhando o tráfego da Internet para seus recursos AWS.

Roteamento avançado de DNS

- Ao usar roteamento por geolocalização, por geoproximidade ou encaminhamento por latência, sempre defina um padrão, a menos que queira que alguns clientes recebam respostas sem resposta.
- Para minimizar a latência da aplicação, use o encaminhamento por latência. Esse tipo de dados de roteamento pode ser alterado com frequência.
- Para fornecer estabilidade e previsibilidade de roteamento, use roteamento por geolocalização ou por geoproximidade.

Para obter mais informações, consulte Roteamento de localização geográfica, Roteamento por geoproximidade e Roteamento baseado em latência.

Propagação das alterações de DNS

Quando você cria ou atualiza um registro ou zona hospedada usando o console ou a API do Route 53, leva algum tempo para alteração ser refletida na Internet. Isso se chama propagação de alterações. Embora normalmente a propagação demore menos de um minuto globalmente, existem atrasos ocasionais, por exemplo, devido a problemas de sincronização com um local ou, em casos raros, problemas dentro do plano de controle central. Se você estiver criando fluxos de trabalho de provisionamento automatizado e for importante aguardar a conclusão da propagação das alterações antes de prosseguir com a próxima etapa do fluxo de trabalho, use a GetChangeAPI para verificar se as alterações de DNS entraram em vigor (). `Status =INSYNC`

Delegação de DNS

Ao delegar vários níveis de subdomínios no DNS, é importante sempre delegar da zona pai. Por exemplo, se você estiver delegando www.dept.example.com, deverá fazê-lo a partir da zona dept.example.com, e não da zonaexample.com. As delegações de uma zona avô para uma zona filho pode não funcionar de modo algum ou funcionar apenas de forma inconsistente. Para ter mais informações, consulte Rotear tráfego para subdomínios.

Tamanho da resposta do DNS

Evite criar respostas únicas e grandes. Se as respostas forem maiores que 512 bytes, muitos resolvedores DNS devem tentar novamente por TCP em vez de UDP, o que pode reduzir a confiabilidade e levar a respostas mais lentas. Recomendamos usar o roteamento de resposta de vários valores, que escolhe oito endereços IP aleatórios íntegros para manter as respostas dentro do limite de 512 bytes.

Para obter mais informações, consulte Roteamento de resposta com vários valores e DNS Reply Size Test Server (Servidor de teste de tamanho de respostas de DNS).

Práticas recomendadas do Resolver

Siga estas práticas recomendadas para otimizar o Route 53 Resolver.

Tópicos

- Evite configurações de loop com endpoints do Resolver
- Escalabilidade de endpoints do Resolver
- Alta disponibilidade de endpoints do Resolver
- Deslocamento de zona DNS

Evite configurações de loop com endpoints do Resolver

Não associe a mesma VPC a uma regra do Resolver e seu endpoint de entrada (seja um destino direto do endpoint, seja por meio de um servidor DNS on-premises). Quando o endpoint de saída em uma regra do Resolver apontar para um endpoint de entrada que compartilha uma VPC com a regra, ele pode causar um loop em que a consulta é transmitida continuamente entre os endpoints de entrada e de saída.

A regra de encaminhamento ainda pode ser associada a outras VPCs que são compartilhadas com outras contas usando AWS Resource Access Manager ()AWS RAM. Zonas hospedadas privadas associadas ao hub, ou a uma VPC central, ainda serão resolvidas de consultas para endpoints de entrada porque uma regra do resolvedor de encaminhamento não altera essa resolução.

Escalabilidade de endpoints do Resolver

Os grupos de segurança de endpoint do Resolver usam o acompanhamento da conexão para coletar informações sobre o tráfego de entrada e saída dos endpoints. Cada interface do endpoint tem um número máximo de conexões que podem ser rastreadas, e um alto volume de consultas de DNS pode exceder as conexões e causar controle de utilização e perda de consulta. Para reduzir o número de conexões que são rastreadas, implemente regras do grupo de segurança que permitem o tráfego com base no estado de conexão do tráfego. Para obter mais informações, consulte Grupos de segurança e rastreamento de conexão no Guia do usuário do Amazon EC2.

As conexões feitas por meio de aplicativos como o Network Load Balancer e AWS Lambda (para obter uma lista completa, consulte Conexões rastreadas automaticamente) são rastreadas automaticamente, mesmo que a configuração do grupo de segurança não exija rastreamento.

Se o rastreamento de conexão for aplicado usando regras restritivas de grupos de segurança ou se as consultas forem roteadas por meio do Network Load Balancer, o máximo geral de consultas por segundo por endereço IP para um endpoint de entrada poderá ser tão baixo quanto 1500.

Recomendações de grupo de segurança do Resolver de entrada e saída

Regras de entrada		
Tipo de protocolo	Número da porta	IP de origem
TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0
Regras de saída		
Tipo de protocolo	Número da porta	IP de destino
TCP	Todos	0.0.0.0/0
UDP	Todos	0.0.0.0/0

Endpoints do Resolver de entrada

Para clientes que usam um endpoint do Resolver de entrada, a capacidade da interface de rede elástica será afetada se você tiver mais de 40.000 combinações exclusivas de endereços IP e portas gerando o tráfego DNS.

Alta disponibilidade de endpoints do Resolver

Quando você cria seus endpoints de entrada do Route 53 Resolver, o Route 53 requer que você crie pelo menos dois endereços IP para os quais os resolvedores de DNS na rede encaminharão consultas. Também é necessário especificar o endereço IP em pelo menos duas zonas de disponibilidade para obter redundância.

Se você precisar que mais de um endpoint da interface de rede elástica esteja disponível o tempo todo, recomendamos que você crie pelo menos uma interface de rede a mais do que a necessária, para garantir que você tenha capacidade adicional disponível para lidar com possíveis picos de tráfego. A interface de rede adicional também garante a disponibilidade durante as operações de serviço, como manutenção ou atualizações.

Para ter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada.

Deslocamento de zona DNS

Um ataque de deslocamento de zona DNS tenta obter todo o conteúdo de zonas DNS assinadas pelo DNSSEC. Se a equipe do Route 53 Resolver detectar um padrão de tráfego que corresponda aos gerados quando as zonas DNS são percorridas em seu endpoint, a equipe de serviço acelerará o tráfego no endpoint. Como consequência, você pode observar uma porcentagem alta de suas consultas de DNS expirando.

Se você observar capacidade reduzida em seus endpoints e acreditar que o endpoint foi controlado erroneamente, acesse https://console.aws.amazon.com/support/home#/ para criar um caso de suporte.

Práticas recomendadas para verificações de integridade do Amazon Route 53

Siga estas práticas recomendadas para otimizar as verificações de integridade do Amazon Route 53.

Tópicos

- Práticas recomendadas para endereços de IP elástico para verificações de integridade

Práticas recomendadas para endereços de IP elástico para verificações de integridade

A prática recomendada para seus endpoints de verificação de integridade é usar endereços de IP elástico. No entanto, certifique-se de excluir qualquer verificação de integridade associada a um endereço de IP elástico que você não possui mais. Por exemplo, se você não estiver mais usando uma instância do Amazon EC2, certifique-se de excluir qualquer verificação de integridade associada ao endereço de IP elástico. Isso ocorre porque o endereço IP elástico pode ser atribuído a um usuário diferente ou Conta da AWS, o que pode comprometer seus dados de verificação de saúde.

Cotas

As solicitações e entidades da API do Amazon Route 53 estão sujeitas às cotas a seguir (anteriormente chamadas de “limites”).

Tópicos

Como usar o Service Quotas para visualizar e gerenciar cotas

É possível usar o serviço Service Quotas para visualizar cotas e solicitar aumentos de cota para muitos produtos da AWS . Para obter mais informações, consulte o Manual do usuário do Service Quotas. (No momento, você pode usar o Service Quotas para visualizar e gerenciar domínios, Route 53 e cotas do Route 53 Resolver).

> **Note**
>
> Para visualizar cotas e solicitar cotas mais altas para o Route 53, altere a região para Leste dos EUA (Norte da Virgínia). Para visualizar cotas e solicitar cotas mais altas para o Resolver, altere para a região aplicável.

Cotas em entidades

As entidades do Amazon Route 53 estão sujeitas às cotas a seguir.

Para obter informações sobre como obter cotas atuais (anteriormente chamadas de “limites”), consulte as seguintes ações do Route 53:

- GetAccountLimite — Obtém cotas em verificações de saúde, zonas hospedadas, conjuntos de delegações reutilizáveis, políticas de fluxo de tráfego e registros de políticas de fluxo de tráfego
- GetHostedZoneLimit— Obtém cotas em registros em uma zona hospedada e em Amazon VPCs que você pode associar a uma zona hospedada privada

- GetReusableDelegationSetLimite — Obtém a cota do número de zonas hospedadas que você pode associar a um conjunto de delegações reutilizáveis

Tópicos

Cotas em domínios

Entidade	Cota
Domínios	20* por conta AWS Solicite uma cota maior.

*O limite é de 20 para novos clientes desde março de 2021.

Se você tiver uma conta existente e seu limite padrão for 50 agora, ela permanecerá em 50.

Cotas em zonas hospedadas

Entidade	Cota
Zonas hospedadas	Cota inicial de 500 por AWS conta, mas você pode solicitar uma cota maior conforme necessário.

Entidade	Cota
	Solicite uma cota maior.
Zonas hospedadas que podem usar o mesmo conjunto de delegações reutilizáveis	100 Solicite uma cota maior.
VPCs da Amazon que você pode associar a uma zona hospedada privada por zona hospedada	300 Solicite uma cota maior.
As zonas hospedadas privadas que você pode associar a uma VPC	Sem cota *.
Autorizações que você pode criar para associar as VPCs criadas por uma conta a uma zona hospedada criada por outra conta	1000
O número de chaves de assinatura de chave (KSK) que você pode criar por zona hospedada	2

* Você pode associar uma VPC a qualquer uma ou a todas as zonas hospedadas privadas que você controla por meio de suas AWS contas. Por exemplo, suponha que você tenha três AWS contas e todas as três tenham a cota padrão de 500 zonas hospedadas. Se você criar 500 zonas hospedadas privadas para todas as três contas, poderá associar uma VPC a todas as 1.500 zonas hospedadas privadas.

Cotas em registros

Entidade	Cota

Entidade	Cota
Registros	10.000 por zona hospedada Solicite uma cota maior. Para uma cota superior a 10 mil registros em uma zona hospedada, aplica-se uma cobrança adicional. Para obter mais informações, consulte Preço do Amazon Route 53.
Recordes em um conjunto de registros	400 por conjunto de registros
Registros de geolocalização, latência, resposta multivalor e baseados em IP	100 registros que têm o mesmo nome e tipo
Registros de geoproximidade	30 registros que têm o mesmo nome e tipo
Coleções CIDR	5 por Conta da AWS. Solicite uma cota maior.
Blocos CIDR	1000 por coleção CIDR. Solicite uma cota maior.

Cotas no Route 53 Resolver

Esta seção inclui todas as cotas do Route 53 Resolver

Cotas no Route 53 Resolver

Use o procedimento a seguir para aumentar as cotas para o Route 53 Resolver.

Para aumentar as cotas do Resolver

1. Abra o console do Service Quotas em https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas.

2. Vá para a região na qual você deseja aumentar o limite.
3. Selecione o Quota name (Nome da cota) do Route 53 Resolver que você deseja aumentar.
4. Selecione Request quota increase (Solicitar aumenta da cota), insira o valor da cota e selecione Request (Solicitar).

Cotas nos endpoints do Route 53 Resolver

Entidade	Cota
Endpoints por região AWS	4 por AWS conta Solicite uma cota maior.
Endereços IP por endpoint	6 Solicite uma cota maior.
Endereços IP por regra	6
Regras por AWS região	1000 por AWS conta Solicite uma cota maior.
Associações entre regras e VPCs por região AWS	2000 por AWS conta Solicite uma cota maior.
Consultas UDP por segundo por endereço IP em um endpoint	10.000*

* Cada endereço IP em um endpoint pode processar até 10.000 consultas DNS UDP por segundo (QPS). O número de QPS de DNS varia de acordo com o tipo de consulta, tamanho da resposta, integridade dos servidores de nome de destino, tempos de resposta de consultas, latência de ida e

volta, e o protocolo em uso. Por exemplo, consultas a um servidor de nome de destino lento para responder podem reduzir significativamente a capacidade da interface de rede. Além disso, para garantir alta disponibilidade, o Route 53 Resolver gera consultas de saída redundantes para cada solicitação de DNS que recebe. Como resultado, o QPS para cada interface de rede de saída não corresponderá ao QPS enviado para o Route 53 Resolver. Use CloudWatch métricas para medir quantas consultas estão sendo enviadas para cada interface de rede. Para ter mais informações, consulte Métricas para endereços IP do Resolver . Se a taxa máxima de consulta exceder 50% da capacidade de qualquer interface de rede no endpoint, você poderá adicionar mais interfaces de rede para aumentar a capacidade do endpoint.

As conexões feitas por meio de aplicativos como o Network Load Balancer e AWS Lambda (para obter uma lista completa, consulte Conexões rastreadas automaticamente) são rastreadas automaticamente, mesmo que a configuração do grupo de segurança não exija rastreamento.

Se o rastreamento de conexão for aplicado usando regras restritivas de grupos de segurança ou se as consultas forem roteadas por meio do Network Load Balancer, o máximo geral de consultas por segundo por endereço IP para um endpoint de entrada poderá ser tão baixo quanto 1500.

Cotas nos logs de consulta do Route 53 Resolver

Entidade	Cota
Configurações de log de consulta por região AWS	20
Associações da VPC de configuração de log de consultas por AWS *	100
Associações de VPC de configuração de log de consulta por Região AWS (compartilhada usando RAM) da conta com a qual a configuração foi compartilhada.	100

* Esse é um limite fixo. Você não pode criar outra configuração de log de consulta na mesma Região da AWS e associar 100 VPCs adicionais a ela.

Cotas no Firewall de DNS do Route 53 Resolver

Entidade	Cota
Número de grupos de regras associados a uma VPC para uma única conta por região da AWS	5
Número de domínios de firewall DNS em um único arquivo Amazon S3 para uma única conta por região AWS	250.000 Solicite uma cota maior.
Número de grupos de regras de firewall DNS para uma única conta por região AWS	1.000 Solicite uma cota maior.
Número de regras em um grupo de regras para uma única conta por AWS região	100 Solicite uma cota maior.
Número de listas de domínio para uma única conta por AWS região	1000 Solicite uma cota maior.
O número máximo de domínios que você pode especificar em todas as listas de domínios para uma única conta por região AWS	100.000 Solicite uma cota maior.

Cotas do Resolver no Outpost

Entidade	Cota

Entidade	Cota
Limite de instâncias do Resolver no Outpost	6 (sendo obrigatório um mínimo de 4)

Os tipos de instância do Resolver on Outpost e o número de consultas de DNS por segundo que cada tipo de instância pode acomodar:

Tipo de instância	Consultas por segundo
c5.large	Até 7.000
c5.xlarge	Até 12.000
c5.2xlarge	Até 24.000
c5.4xlarge	Até 56.000
c5d.large	Até 7.000
c5d.xlarge	Até 12.000
c5d.2xlarge	Até 24.000
c5d.4xlarge	Até 56.000
m5.large	Até 7.000
m5.xlarge	Até 12.000
m5.2xlarge	Até 24.000
m5.4xlarge	Até 56.000

Tipo de instância	Consultas por segundo
m5d.large	Até 7.000
m5d.xlarge	Até 12.000
m5d.2xlarge	Até 24.000
m5d.4xlarge	Até 56.000
r5.large	Até 7.000
r5.xlarge	Até 12.000
r5.2xlarge	Até 24.000
r5.4xlarge	Até 56.000
r5d.large	Até 7.000
r5d.xlarge	Até 12.000
r5d.2xlarge	Até 24.000
r5d.4xlarge	Até 56.000

Os tipos de instância de endpoint do Resolver on Outpost e o número de consultas de DNS por segundo que cada tipo de instância pode acomodar:

Tipo de instância	Consultas por segundo

Tipo de instância	Consultas por segundo
c5.large	Até 5.000
c5.xlarge	Até 10 mil
c5.2xlarge	Até 18.000
c5.4xlarge	Até 30.000
c5d.large	Até 5.000
c5d.xlarge	Até 10 mil
c5d.2xlarge	Até 18.000
c5d.4xlarge	Até 30.000
m5.large	Até 5.000
m5.xlarge	Até 10 mil
m5.2xlarge	Até 18.000
m5.4xlarge	Até 30.000
m5d.large	Até 5.000
m5d.xlarge	Até 10 mil
m5d.2xlarge	Até 18.000

Tipo de instância	Consultas por segundo
m5d.4xlarge	Até 30.000
r5.large	Até 5.000
r5.xlarge	Até 10 mil
r5.2xlarge	Até 18.000
r5.4xlarge	Até 30.000
r5d.large	Até 5.000
r5d.xlarge	Até 10 mil
r5d.2xlarge	Até 18.000
r5d.4xlarge	Até 30.000

Cotas em verificações de integridade

Entidade	Cota
Verificações de integridade	200 verificações de saúde ativas por AWS conta Solicite uma cota maior.
Verificações de integridade secundárias que uma verificação de integridade calculada pode monitorar	255

Entidade	Cota
Tamanho total máximo de cabeçalhos na resposta a uma solicitação de verificação de integridade	16.384 bytes (16K)

Cotas em configurações de log de consultas

Entidade	Cota
Configurações do log de consultas	1 por zona hospedada

Cotas em políticas de fluxo de tráfego e registros de políticas

Entidade	Cota
Políticas de tráfego Para obter mais informações sobre o fluxo de tráfego do Route 53, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS.	50 por AWS conta Solicite uma cota maior.
Versões das políticas de tráfego	1000 por política de tráfego
Registros de política de tráfego (chamados de “instâncias de política” na API, nos SDKs e AWS Tools for Windows PowerShell nos AWS SDKs do Route 53) AWS Command Line Interface	5 por AWS conta Solicite uma cota maior.

Cotas em conjuntos de delegações reutilizáveis

Entidade	Cota
Conjuntos de delegações reutilizáveis	100 por AWS conta Solicite uma cota maior.

Cotas nos perfis do Route 53

Entidade	Cota
Número de perfis do Route 53 por Conta da AWS região	5 Solicite uma cota maior.
Número de VPCs que podem ser associadas a um perfil	1000 Solicite uma cota maior.
Número de grupos de regras do DNS Firewall por perfil	5
Número de regras do Resolver por perfil	1000 Solicite uma cota maior.
Número de zonas hospedadas privadas por perfil	1.000 Solicite uma cota maior.

Máximos em solicitações de API

As solicitações de API do Amazon Route 53 estão sujeitas aos números máximos a seguir.

Tópicos

Número de elementos e caracteres nas solicitações **`ChangeResourceRecordSets`**

Elementos **`ResourceRecord`**

Uma solicitação não pode conter mais de mil elementos `ResourceRecord` (incluindo registros de alias). Quando o valor do elemento `Action` é `UPSERT`, cada elemento `ResourceRecord` é contado duas vezes.

Número máximo de caracteres

A soma do número de caracteres (incluindo espaços) em todos os elementos `Value` de uma solicitação não pode exceder 32.000 caracteres. Quando o valor do elemento `Action` é `UPSERT`, cada caractere em um elemento `Value` é contado duas vezes.

Frequência das solicitações de API do Amazon Route 53

Todas as solicitações de API do Amazon Route 53

Para as APIs do Amazon Route 53, cinco solicitações por segundo por AWS conta. Se você enviar mais de cinco solicitações por segundo, o Amazon Route 53 retornará um erro HTTP 400 (`Bad request`). O cabeçalho de resposta também inclui um elemento `Code` com um valor de `Throttling` e um elemento `Message` com um valor de `Rate exceeded`.

> **Note**
>
> Se o seu aplicativo exceder esse limite, recomendamos que você implemente o recuo exponencial para novas tentativas. Para ter mais informações, consulte Repetições de erro e recuo exponencial na AWS no Referência geral da Amazon Web Services.

Solicitações **`ChangeResourceRecordSets`**

Se o Route 53 não puder processar uma solicitação antes da próxima solicitação chegar, ele rejeitará as solicitações subsequentes para a mesma zona hospedada e retornará um erro HTTP 400 (`Bad request`). O cabeçalho de resposta também incluirá um elemento `Code` com um valor de `PriorRequestNotComplete` e um elemento `Message` com um valor de `The request was rejected because Route 53 was still processing a prior request.`

Solicitações **`CreateHealthCheck`**

Você pode enviar uma `CreateHealthCheck` solicitação a cada 2 segundos por Conta da AWS.

Frequência de solicitações de API do Route 53 Resolver

Todas as solicitações

Cinco solicitações por segundo por AWS conta por região. Se você enviar mais de cinco solicitações por segundo em uma região, o Resolver retornará um erro HTTP 400 (`Bad request`). O cabeçalho de resposta também inclui um elemento `Code` com um valor de `Throttling` e um elemento `Message` com um valor de `Rate exceeded`.

> **Note**
>
> Se o seu aplicativo exceder esse limite, recomendamos que você implemente o recuo exponencial para novas tentativas. Para ter mais informações, consulte Repetições de erro e recuo exponencial na AWS no Referência geral da Amazon Web Services.

Informações relacionadas

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

Tópicos

- Recursos do AWS
- Ferramentas e bibliotecas de terceiros
- Interfaces gráficas do usuário

Recursos do AWS

Vários guias úteis, fóruns e outros recursos estão disponíveis na Amazon Web Services.

- Referência da API do Amazon Route 53: um guia de referência que inclui o local do esquema, descrições completas das ações da API, parâmetros e tipos de dados e uma lista dos erros que o serviço retorna.
- Tipo de AWS::Route53::RecordSet no Manual do usuário do AWS CloudFormation: uma propriedade para usar o Amazon Route 53 com o AWS CloudFormation para criar nomes DNS personalizados para suas pilhas do AWS CloudFormation.
- Fóruns de discussão: um fórum comunitário para desenvolvedores discutirem questões técnicas relacionadas ao Route 53.
- AWS Support Center: este site reúne informações sobre seus casos de suporte e resultados recentes do Trusted Advisor da AWS e de verificações de integridade, além de fornecer links para fóruns de discussão, perguntas técnicas frequentes, o painel de integridade de serviços e informações sobre os planos de suporte da AWS.
- Informações do Premium Support da AWS: a principal página da Web para obter informações sobre o Premium Support da AWS, um canal de suporte de resposta rápida e com atendimento individual para ajudar você a criar e executar aplicações nos serviços de infraestrutura da AWS.
- Entre em contato conosco: links para consultas sobre sua conta ou faturamento. Para dúvidas técnicas, use os fóruns de discussão ou links de suporte acima.
- Informações sobre o produto Route 53: a principal página da Web para obter informações sobre o Route 53, incluindo recursos, preços e muito mais.

- Aulas e workshops — Links para cursos de especialidades e baseados em perfil, bem como laboratórios autoguiados para ajudar a aperfeiçoar suas habilidades na AWS e a obter experiência prática.
- Centro dos desenvolvedores da AWS — Explore tutoriais, baixe ferramentas e informe-se sobre eventos para desenvolvedores da AWS.
- Ferramentas do desenvolvedor da AWS — Links para ferramentas de desenvolvedor, SDKs, toolkits de IDE e ferramentas da linha de comando para desenvolver e gerenciar aplicativos da AWS.
- Centro de recursos de conceitos básicos — Saiba como configurar a Conta da AWS, participar da comunidade da AWS e lançar seu primeiro aplicativo.
- Tutoriais práticos — Siga os tutoriais passo a passo para iniciar seu primeiro aplicativo na AWS.
- Whitepapers da AWS — Links para uma lista abrangente de whitepapers técnicos da AWS que abrangem tópicos como arquitetura, segurança e economia, elaborados pelos arquitetos de soluções da AWS ou por outros especialistas técnicos.
- AWS Support Center: a central para criar e gerenciar seus casos do AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e AWS Trusted Advisor.
- AWS Support — A página Web principal para obter informações sobre o AWS Support, um canal de suporte de resposta rápida e com atendimento individual para ajudar a construir e a executar aplicativos na nuvem.
- Entrar em contato – Um ponto central de contato para consultas relativas a faturas da AWS, contas, eventos, uso abusivo e outros problemas.
- Termos do site da AWS: informações detalhadas sobre nossos direitos autorais e marca registrada; sua conta, licença e acesso ao site, entre outros tópicos.

Ferramentas e bibliotecas de terceiros

Além dos recursos da AWS, você pode encontrar várias ferramentas e bibliotecas de terceiros que funcionam com o Amazon Route 53.

- AmazonRoute53AppsScript (via webos-goodies)

  Gerenciamento de planilhas do Google do Amazon Route 53.
- AWSComponente do .NET (via SprightlySoft)

Componente SprightlySoft .NET para a Amazon Web Services com suporte às operações REST e ao Route 53.

- Download da API do Boto (via github)

  Interface do Boto Python para a Amazon Web Services.

- cli53 (via github)

  Interface da linha de comando do Route 53.

- API do Dasein Cloud

  API baseada em Java.

- R53.py (via github)

  Mantém uma versão canônica das suas configurações de DNS sob controle de origem e calcula o conjunto mínimo de mudanças necessárias para alterar uma configuração.

- route53d

  Front-end de DNS para a API do Route 53 (permite a transferência de zona incremental [IXFR]).

- Route53Manager (via github)

  Interface baseada na web.

- Ruby Fog (via github)

  A biblioteca de serviços em nuvem do Ruby.

- WebService::Amazon::Route53 (via CPAN)

  Interface Perl com a API do Amazon Route 53.

Interfaces gráficas do usuário

As seguintes ferramentas de terceiros fornecem interfaces gráficas de usuário (GUIs) para uso com o Amazon Route 53:

- R53 Fox
- Ylastic

Histórico do documento

As entradas a seguir descrevem as alterações importantes feitas em cada versão da documentação do Route 53. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Tópicos

Lançamentos de 2024

30 de abril de 2024

Agora você pode decidir se uma regra de firewall de DNS inspecionará (padrão) ou confiará na cadeia de redirecionamento de DNS. Para obter mais informações, consulte Componentes e configurações do Firewall DNS do Route 53 Resolver e Configurações de regra no Firewall DNS.

22 de abril de 2024

Agora você pode usar os Perfis do Route 53 para compartilhar configurações específicas de DNS com várias VPCs e com contas. AWS Para ter mais informações, consulte Perfis do Amazon Route 53.

22 de abril de 2024

Foram adicionadas as políticas gerenciadas `AmazonRoute53ProfilesReadOnlyAccess` e concederam `AmazonRoute53ProfilesFullAccess` acesso total e somente para leitura aos perfis do Amazon Route 53. Para ter mais informações, consulte AWS políticas gerenciadas para o Amazon Route 53.

5 de fevereiro de 2024

Agora você pode usar a Amazon EventBridge para alertas em tempo real com o DNS Firewall. Para ter mais informações, consulte Gerenciando eventos do Route 53 Resolver DNS Firewall usando Amazon EventBridge.

9 de janeiro de 2024

Agora você pode usar o tipo de consulta DNS como um valor opcional para a regra de firewall DNS para diferenciar a resposta da regra para um tipo específico de consulta DNS. Para obter mais informações, consulte Componentes e configurações do Firewall DNS do Route 53 Resolver e Configurações de regra no Firewall DNS.

9 de janeiro de 2024

Agora você pode usar o registro de criação rápida ou o assistente de criação de registro para criar registros de roteamento por geoproximidade. Para obter mais informações, consulte Roteamento por geoproximidade, Valores específicos para registros de geoproximidade e Valores específicos para registros de alias de geoproximidade.

Lançamentos de 2023

20 de dezembro de 2023

Agora você pode usar o DNS por HTTPS com os endpoints do Route 53 Resolver. Para ter mais informações, consulte Escolher protocolos para os endpoints.

20 de julho de 2023

O Amazon Route 53 on Outposts agora está disponível em racks. AWS Outposts Ele inclui um Resolver que armazena em cache todas as consultas ao DNS oriundas do AWS Outposts. É possível também configurar conectividade híbrida entre um Outpost e um resolver de DNS on-premises quando você implanta endpoints de entrada e de saída. Para ter mais informações, consulte O que é o Amazon Route 53 no Outposts?.

19 de julho de 2023

Agora você pode usar as zonas locais com roteamento por geoproximidade (fluxo de tráfego apenas) depois de habilitá-las. Para obter mais informações, consulte Roteamento por geoproximidade e Formato do documento de política de tráfego.

22 de março de 2023

Atualizado todo o guia do Route 53 com a nova experiência de console para domínios. Você também pode usar a nova experiência do console para transferir um domínio de um Conta da AWS para outro Conta da AWS. Para obter mais informações, consulte Registrar um novo domínio e Transferir domínios.

10 de março de 2023

Agora você pode se conectar aos seus recursos usando endpoints IPv4, IPv6 ou de pilha dupla com o Amazon Route 53 Resolver. Para obter mais informações, consulte Valores especificados ao criar ou editar endpoints de entrada e Valores especificados ao criar ou editar endpoints de saída.

Versões de 2022

21 de setembro de 2022

Agora você pode usar condições de política para conceder aos usuários acesso refinado à atualização de conjuntos de registros de recursos no Amazon Route 53. Para ter mais informações, consulte Permissões do conjunto de registros de recursos.

30 de agosto de 2022

O Amazon Route 53 agora oferece suporte a registros de alias para AWS App Runner serviços criados após 1º de agosto de 2022. Para ter mais informações, consulte Roteamento do tráfego para um serviço AWS App Runner.

1º de junho de 2022

A opção de roteamento baseado em IP agora está disponível no Amazon Route 53. Para ter mais informações, consulte Roteamento baseado em IP.

16 de março de 2022

Agora há suporte para opções de roteamento por geolocalização e encaminhamento por latência para zonas hospedadas privadas no Amazon Route 53. Para ter mais informações, consulte Supported routing policies for records in a private hosted zone.

25 de janeiro de 2022

O processo para alterar a propriedade para TLDs .com.au e .net.au foi simplificado para incluir a resposta a dois e-mails (por registrantes novos e antigos) e não inclui o preenchimento de formulários. Para obter mais informações, consulte .com.au (Austrália) e .net.au (Austrália).

Versões de 2021

26 de outubro de 2021

Suporte adicionado para desabilitar regras padrão de DNS reverso com o Amazon Route 53. Agora, é possível desabilitar a criação dessas regras e, em vez disso, direcionar consultas de namespaces de DNS reverso para servidores externos conforme desejado. Para ter mais informações, consulte Regras de encaminhamento para consultas DNS reversas no Resolver.

1º de setembro de 2021

Foi adicionado um novo tópico de introdução que orienta você na criação de CloudFront distribuições da Amazon para um site estático. Para ter mais informações, consulte Use uma CloudFront distribuição da Amazon para servir um site estático.

14 de julho de 2021

Começou a rastrear políticas AWS gerenciadas para o Amazon Route 53. Para ter mais informações, consulte AWS políticas gerenciadas para o Amazon Route 53.

31 de março de 2021

Adicionado Firewall DNS do Route 53 Resolver. Com o Firewall DNS, você pode fornecer proteção para solicitações DNS de saída de suas VPCs. Para ter mais informações, consulte Firewall de DNS do Route 53 Resolver.

Versões de 2020

17 de dezembro de 2020

Adicionado suporte para assinatura de DNSSEC para o Route 53 Resolver. Para ter mais informações, consulte Como configurar a assinatura de DNSSEC no Amazon Route 53.

Adicionado suporte para validação de DNSSEC para o Route 53 Resolver. Para ter mais informações, consulte Como habilitar validação de DNSSEC no Amazon Route 53.

23 de setembro de 2020

Atualizamos todo o guia do Route 53 com a nova experiência do console. Para ter mais informações, consulte O que é o Amazon Route 53?.

1.º de setembro de 2020

Adicionado suporte para logs de consulta do Resolver. Para ter mais informações, consulte Log de consultas do Resolver.

Versões de 2018

20 de dezembro de 2018

Você pode criar registros de alias do Route 53 que encaminham o tráfego para as APIs do API Gateway ou para os endpoints da interface da Amazon VPC. Para ter mais informações, consulte Valor/rotear tráfego para.

28 de novembro de 2018

O Route 53 Auto Naming (também conhecido como Service Discovery) agora é um serviço separado, AWS Cloud Map. Para mais informações, consulte o Guia do desenvolvedor do AWS Cloud Map.

19 de novembro de 2018

Você também pode usar o resolvedor do Route 53 para configurar a resolução de DNS entre a VPC e a rede por meio de uma conexão VPN ou do Direct Connect: (Resolver é o novo nome para o serviço DNS recursivo que é fornecido para todos os clientes por padrão na Amazon Virtual Private Cloud [Amazon VPC].) Isso permite que você encaminhe consultas de DNS de resolvedores em sua rede para o Route 53 Resolver. O resolvedor também permite que você

encaminhe consultas de determinados nomes de domínio (example.com) e nomes de subdomínio (api.example.com) de uma VPC para os resolvedores na rede. Para ter mais informações, consulte O que Amazon Route 53 Resolveré.

7 de novembro de 2018

Quando você estiver usando o fluxo de tráfego e o roteamento de geoproximity do Route 53, é possível usar um mapa interativo para visualizar como seus usuários finais serão roteados para seus endpoints em todo o mundo. Para ter mais informações, consulte Visualizar um mapa que mostra o efeito das configurações de geoproximidade.

18 de outubro de 2018

Você pode usar a API e o console do Route 53 para desabilitar temporariamente uma verificação de integridade do Route 53. Isso oferece uma maneira fácil de pausar o monitoramento de um endpoint, como um servidor web, para que você possa fazer manutenção nele sem acionar alarmes nem gerar mensagens de status ou logs desnecessários. Para obter mais informações, consulte "Desabilitado" em Valores que você especifica quando cria ou atualiza uma verificação de integridade. O recurso está disponível para todos os três tipos de verificações de saúde do Route 53: verificações de saúde que monitoram um endpoint, verificações de saúde que monitoram outras verificações de saúde e verificações de saúde que monitoram um CloudWatch alarme.

13 de março de 2018

Se você usa a nomenclatura automática, agora pode usar um verificador de integridade de terceiros para avaliar a integridade dos seus recursos. Isso é útil quando um recurso não está disponível na Internet, por exemplo, porque a instância está em uma Amazon VPC. Para obter mais informações, consulte HealthCheckCustomConfiga Referência de API do Amazon Route 53.

9 de março de 2018

Agora o IAM inclui políticas gerenciadas para nomenclatura automática. Para ter mais informações, consulte AWS políticas gerenciadas para o Amazon Route 53.

6 de fevereiro de 2018

Agora você pode configurar a nomenclatura automática para criar registros de alias que roteiam o tráfego para load balancers ELB ou para criar registros CNAME. Para obter mais informações, consulte Atributos na documentação da RegisterInstanceAPI na Referência de API do Amazon Route 53.

Versões de 2017

5 de dezembro de 2017

Agora você pode usar a API de nomeação automática do Route 53 para provisionar instâncias para microsserviços. A nomeação automática permite que você crie automaticamente registros DNS e, se desejar, verificações de integridade com base em um modelo que definir. Para obter mais informações, consulte O que é o AWS Cloud Map? no Guia do AWS Cloud Map desenvolvedor.

16 de novembro de 2017

Agora é possível obter de forma programática as cotas atuais para recursos do Route 53, como zonas hospedadas e verificações de integridade, e o número de cada recurso que você está usando no momento. Para obter mais informações, consulte GetAccountLimitGetHostedZoneLimit, e GetReusableDelegationSetLimitna Referência de API do Amazon Route 53.

3 de outubro de 2017

O Route 53 agora é um serviço qualificado da HIPAA. Para ter mais informações, consulte Validação de conformidade do Amazon Route 53.

29 de setembro de 2017

Agora você pode verificar programaticamente se um domínio pode ser transferido para o Route 53. Para obter mais informações, consulte CheckDomainTransferabilitya Referência de API do Amazon Route 53.

11 de setembro de 2017

Agora você pode criar registros de alias do Route 53 que encaminharam o tráfego da Internet para os balanceadores de carga da rede do Elastic Load Balancing. Para obter mais informações sobre registros com alias, consulte Escolher entre registros de alias e não alias.

7 de setembro de 2017

Se você estiver usando o Route 53 como seu serviço DNS autoritativo e público, poderá registrar as consultas DNS que o Route 53 recebe. Para ter mais informações, consulte Log de consultas de DNS pública.

1 de setembro de 2017

Se você estiver usando o fluxo de tráfego do Route 53, poderá usar o roteamento de proximidade geográfica, o que permite encaminhar o tráfego com base na distância física entre seus usuários e seus recursos. Você também pode rotear mais ou menos tráfego para cada recurso, especificando um desvio positivo ou negativo. Para ter mais informações, consulte Roteamento por geoproximidade.

21 de agosto de 2017

Agora você pode usar o Route 53 para criar registros de Autorização da Autoridade de Certificação (CAA), que permitem especificar as autoridades de certificação que podem emitir certificados para seus domínios e subdomínios. Para ter mais informações, consulte Tipo de registro CAA.

18 de agosto de 2017

Agora você pode transferir uma grande quantidade de domínios para o Route 53 usando o console do Route 53. Para ter mais informações, consulte Como transferir registro de um domínio para o Amazon Route 53.

4 de agosto de 2017

Quando você registra um domínio, os registros de alguns domínios de nível superior (TLDs) exigem que você verifique se especificou um endereço de e-mail válido para o contato de registrante. Agora você pode enviar o e-mail de verificação e obter a confirmação de que o endereço de e-mail foi verificado com sucesso durante o processo de registro do domínio. Para ter mais informações, consulte Registrar um novo domínio.

21 de junho de 2017

Se quiser encaminhar o tráfego de forma aproximada e aleatória para vários recursos, como servidores Web, você pode criar um registro de resposta de múltiplos valores para cada recurso e, se desejar, associar uma verificação de integridade do Route 53 a cada registro. O Route 53 responde às consultas de DNS com até oito registros íntegros, em resposta a cada consulta, e oferece respostas diferentes para resolvedores de DNS diferentes. Para ter mais informações, consulte Roteamento de resposta com vários valores.

10 de abril de 2017

Ao usar o console do Route 53 para transferir um registro de domínio para o Route 53, agora é possível escolher uma das seguintes opções para associar os servidores de nomes ao serviço DNS para o domínio com o registro de domínio transferido:

- Use os servidores de nome para uma zona hospedada do Route 53 de sua escolha
- Use os servidores de nome para o serviço de DNS atual do domínio
- Use os servidores de nome que você especificar

O Route 53 automaticamente associará esses servidores de nome ao registro de domínio transferido.

Versões de 2016

21 de novembro de 2016

Agora você pode criar verificações de integridade que usam endereços IPv6 para verificar a integridade dos endpoints. Para ter mais informações, consulte Criar e atualizar verificações de integridade.

15 de novembro de 2016

Agora você pode usar uma ação de API do Route 53 para associar uma Amazon VPC criada com uma conta a uma zona hospedada privada criada com outra conta. Para ter mais informações, consulte Associando uma Amazon VPC e uma zona hospedada privada que você criou com contas diferentes AWS.

30 de agosto de 2016

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Registros do Name Authority Pointer: agora é possível criar registros de NAPTR, que são usados pelas aplicações do Dynamic Delegation Discovery System (DDDS – Sistema de descoberta de delegação dinâmica) para converter um valor em outro ou substituir um valor por outro. Por exemplo, um uso comum é converter números de telefone em SIP URIs. Para ter mais informações, consulte Tipo de registro NAPTR.
- DNS query test tool: agora é possível simular consultas DNS para um registro e ver o valor retornado pelo Route 53. Para os registros de latência e geolocalização, você também pode simular solicitações de um determinado resolvedor de DNS e/ou endereço IP do cliente para descobrir a resposta que o Route 53 retornaria a um cliente com esse resolvedor e/ou endereço IP. Para ter mais informações, consulte Verificar respostas do Route 53 ao DNS.

11 de agosto de 2016

Com essa versão, é possível criar registros de alias que roteiam o tráfego para os Application Load Balancers de ELB. O processo é igual ao dos Classic Load Balancers. Para ter mais informações, consulte Valor/rotear tráfego para.

9 de agosto de 2016

Com essa versão, o Route 53 passa a oferecer suporte ao DNSSEC para registro de domínios. O DNSSEC permite que você proteja seu domínio contra ataques de falsificação de DNS, também conhecidos como ataques. man-in-the-middle Para ter mais informações, consulte Configurar o DNSSEC para um domínio.

7 de julho de 2016

Agora você pode ampliar manualmente o registro de um domínio e registrar um domínio com um período de registro inicial superior ao período de registro mínimo especificado pelo registro. Para ter mais informações, consulte Estender o período de registro de um domínio.

6 de julho de 2016

Se você for um cliente AISPL com um endereço de contato na Índia, agora poderá usar o Route 53 para registrar domínios. Para obter mais informações, consulte Como gerenciar uma conta na Índia.

26 de maio de 2016

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Relatório de faturamento de domínio: agora é possível baixar um relatório que lista todas as cobranças de registro de domínios, por domínio, em um período especificado. O relatório inclui todas as operações de registro de domínio para as quais há uma taxa, incluindo o registro de domínios, a transferência de domínios para o Route 53, a renovação do registro de domínio e (para alguns TLDs) a alteração do proprietário de um domínio. Para obter mais informações, consulte a seguinte documentação do :
  - Console do Route 53: consulte Fazer download de um relatório de faturamento de domínios
  - API do Route 53 — Veja ViewBillingna Referência da API do Amazon Route 53.
- Novos TLDs: agora você pode registrar domínios que têm os seguintes TLDs: .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website e .uk. Para ter mais informações, consulte Domínios que você pode registrar com o Amazon Route 53.

- Novas APIs para registro de domínio: para as operações que exigem confirmação de que o endereço de e-mail do contato do registrante é válido, como o registro de um novo domínio, agora é possível determinar programaticamente se o contato do registrante clicou no link no e-mail de confirmação e, caso contrário, se o link ainda é válido. Você também pode solicitar programaticamente o envio de outro e-mail de confirmação. Para obter mais informações, consulte a documentação a seguir na Referência da API do Amazon Route 53:
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

5 de abril de 2016

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Verificações de saúde com base em CloudWatch métricas — Agora você pode criar verificações de saúde com base no estado do alarme de qualquer CloudWatch métrica. Isso é útil para verificar a integridade dos endpoints que não podem ser acessados por uma verificação de integridade padrão do Route 53, como instâncias em uma Amazon Virtual Private Cloud (VPC) que contêm apenas endereços IP privados. Para obter mais informações, consulte a seguinte documentação do :
  - Console do Route 53: consulte Monitorar um alarme do CloudWatch no tópico “Valores que você especifica ao criar ou atualizar verificações de integridade”.
  - API do Route 53 — Veja CreateHealthChecke UpdateHealthCheckna Referência de API do Amazon Route 53.
- Locais de verificação de integridade configuráveis: agora é possível escolher as regiões de verificação de integridade do Route 53 que verificam a integridade de seus recursos, reduzindo a carga de trabalho no endpoint das verificações de integridade. Isso é útil se seus clientes estiverem concentrados em uma ou poucas regiões geográficas. Para obter mais informações, consulte a seguinte documentação do :
  - Console do Route 53: consulte Health checker regions no tópico “Valores que você especifica ao criar ou atualizar verificações de integridade”.
  - API do Route 53 — Veja o `Regions` elemento de CreateHealthChecke UpdateHealthCheckna Referência de API do Amazon Route 53.
- Failover em zonas hospedadas privadas: agora é possível criar registros com alias e de alias de failover em uma zona hospedada privada. Ao combinar esse recurso com as verificações de integridade baseadas em métricas, é possível configurar o failover de DNS até mesmo para os endpoints que contêm apenas endereços IP privados e não podem ser alcançados

pelas verificações de integridade padrão do Route 53. Para obter mais informações, consulte a seguinte documentação do :

- Console do Route 53: consulte Configurar failover em uma zona hospedada privada.
- API do Route 53 — Veja ChangeResourceRecordSetsna Referência da API do Amazon Route 53.

- Registros com alias em zonas hospedadas privadas: anteriormente, era possível criar registros com alias que encaminhavam consultas DNS somente para outros registros do Route 53 na mesma zona hospedada. Com esta versão, também é possível criar registros com alias que encaminham consultas DNS para ambientes do Elastic Beanstalk com subdomínios regionalizados, para balanceadores de carga do Elastic Load Balancing e buckets do Amazon S3. (Você ainda não pode criar registros de alias que encaminhem consultas de DNS para uma CloudFront distribuição.) Para obter mais informações, consulte a seguinte documentação do :
  - Console do Route 53: consulte Escolher entre registros de alias e não alias.
  - API do Route 53 — Veja ChangeResourceRecordSetsna Referência da API do Amazon Route 53.

23 de fevereiro de 2016

Ao criar ou atualizar as verificações de integridade de HTTPS, agora é possível configurar o Route 53 para enviar o nome de host ao endpoint durante a negociação de TLS. Isso permite que o endpoint responda à solicitação de HTTPS com o certificado SSL/TLS aplicável. Para obter mais informações, consulte a descrição do campo Enable SNI no tópico "Valores que você especifica ao criar ou atualizar verificações de integridade". Para obter informações sobre como habilitar o SNI ao usar a API para criar ou atualizar uma verificação de saúde, consulte CreateHealthCheke UpdateHealthCheckna Referência de API do Amazon Route 53.

27 de janeiro de 2016

Agora é possível registrar domínios para mais de 100 domínios de nível superior (TLDs) adicionais, como .accountants, .band, e .city. Para uma lista completa dos TLDs compatíveis, consulte Domínios que você pode registrar com o Amazon Route 53.

19 de janeiro de 2016

Agora é possível criar registros de alias que encaminham o tráfego para os ambientes do Elastic Beanstalk. Para obter informações sobre como criar registros usando o console do Route 53, consulte Criar registros usando o console do Amazon Route 53. Para obter informações sobre o uso da API para criar registros, consulte ChangeResourceRecordSetsa Referência de API do Amazon Route 53.

Versões de 2015

3 de dezembro de 2015

O console do Route 53 agora inclui um editor visual que permite a criação rápida de configurações de roteamento complexas que usam uma combinação das seguintes políticas de roteamento do Route 53: ponderada, de latência, de failover e de geolocalização. Em seguida, é possível associar a configuração com um ou mais nomes de domínio (como example.com) ou nomes de subdomínio (como www.example.com), na mesma ou em várias zonas hospedadas. Além disso, você poderá reverter as atualizações se a nova configuração não estiver sendo executada conforme o esperado. A mesma funcionalidade está disponível usando a API do Route 53, AWS os SDKs AWS CLI, o e. AWS Tools for Windows PowerShell Para obter informações sobre como usar o editor visual, consulte Usar o fluxo de tráfego para rotear o tráfego de DNS. Para obter informações sobre como usar a API para criar configurações de fluxo de tráfego, consulte a Referência da API do Amazon Route 53.

19 de outubro de 2015

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Registro de domínios .com e .net pelo Amazon Registrar, Inc.: a Amazon agora é registradora credenciada pela ICANN para domínios de nível superior (TLDs) .com e .net pelo Amazon Registrar, Inc. Quando você utilizar o Route 53 para registrar um domínio .com ou .net, o Amazon Registrar será o registrador e ficará listado como o “registrador patrocinador” nos resultados de consulta de Whois. Para obter informações sobre como usar o Route 53 para registrar domínios, consulte Registrar e gerenciar novos domínios com o Amazon Route 53.
- Proteção de privacidade para domínios .com e .net: quando você registra um domínio .com ou .net usando o Route 53, todas as suas informações pessoais, incluindo nome e sobrenome, agora ficam ocultas. O nome e o sobrenome não ficam ocultos em outros domínios registrados com o Route 53. Para obter mais informações sobre proteção de privacidade, consulte Habilitar ou desabilitar a proteção de privacidade para informações de contato de um domínio.

15 de setembro de 2015

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Verificações de integridade calculadas: agora é possível criar verificações de integridade cujos status são determinados pelos status de outras verificações de integridade. Para ter mais informações, consulte Criar e atualizar verificações de integridade. Além disso, consulte CreateHealthCheckna Referência de API do Amazon Route 53.

- Medições de latência para verificações de integridade: agora é possível configurar o Route 53 para medir a latência entre os verificadores de integridade e seu endpoint. Os dados de latência aparecem nos CloudWatch gráficos da Amazon no console do Route 53. Para habilitar a medição de latência nas novas verificações de integridade, consulte a configuração Medições de latência Configuração avançada (somente a opção "Monitorar um endpoint") no tópico Valores que você especifica quando cria ou atualiza uma verificação de integridade. (Não é possível habilitar medições de latência nas verificações de integridade existentes.) Além disso, consulte MeasureLatencyo tópico CreateHealthCheckna Referência de API do Amazon Route 53.
- Atualizações no painel de verificações de saúde no console do Route 53 — O painel para monitorar as verificações de saúde foi aprimorado de várias maneiras, incluindo CloudWatch gráficos para monitorar a latência entre os verificadores de saúde do Route 53 e seus endpoints. Para ter mais informações, consulte Monitorar o status da verificação de integridade e receber notificações.

3 de março de 2015

O Guia do desenvolvedor do Amazon Route 53 agora explica como configurar servidores de nome de rótulo branco para zonas hospedadas do Route 53. Para ter mais informações, consulte Configurar servidores de nome de rótulo branco.

26 de fevereiro de 2015

Agora você pode usar a API do Route 53 para listar as zonas hospedadas associadas a uma AWS conta em ordem alfabética por nome. Você também pode contabilizar as zonas hospedadas associadas a uma conta. Para obter mais informações, consulte ListHostedZonesByNamee GetHostedZoneCountna Referência de API do Amazon Route 53.

11 de fevereiro de 2015

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- Status da verificação de integridade: a página de verificações de integridade no console do Route 53 agora inclui uma coluna Status onde é possível ver o status geral de todas as suas verificações de integridade. Para ter mais informações, consulte Ver o status e o motivo de falhas da verificação de integridade.
- Integração com AWS CloudTrail — O Route 53 agora funciona CloudTrail para capturar informações sobre cada solicitação que sua AWS conta envia para a API do Route 53. A integração do Route 53 CloudTrail permite determinar quais solicitações foram feitas à API do Route 53, o endereço IP de origem do qual cada solicitação foi feita, quem fez a solicitação,

quando ela foi feita e muito mais. Para ter mais informações, consulte Registro de chamadas de API do Amazon Route 53 com AWS CloudTrail.

- Alarmes rápidos para verificações de saúde — Ao criar uma verificação de saúde usando o console do Route 53, agora você pode criar simultaneamente um CloudWatch alarme da Amazon para a verificação de saúde e especificar quem notificar quando o Route 53 considerar o endpoint não íntegro por um minuto. Para ter mais informações, consulte Criar e atualizar verificações de integridade.
- Marcação para zonas hospedadas e domínios: agora é possível atribuir tags que normalmente são usadas para a alocação de custos para domínios e zonas hospedadas do Route 53. Para ter mais informações, consulte Marcação de recursos do Amazon Route 53.

5 de fevereiro de 2015

Agora é possível usar o console do Route 53 para atualizar as informações de contato de um domínio. Para ter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

22 de janeiro de 2015

Agora é possível especificar nomes de domínio internacionalizados ao registrar um novo nome de domínio usando o Route 53. (O Route 53 já oferecia suporte a nomes de domínio internacionalizados nas zonas hospedadas e nos registros.) Para ter mais informações, consulte Formato de nome de domínio DNS.

Versões de 2014

25 de novembro de 2014

Com essa versão, agora é possível editar o comentário que você especificou para uma zona hospedada quando a criou. Para isso, basta clicar no ícone de lápis ao lado do campo Comentário, no console, e inserir um novo valor. Para obter mais informações sobre como alterar o comentário usando a API do Route 53, consulte UpdateHostedZoneCommenta Referência da API do Amazon Route 53.

5 de novembro de 2014

Com esta versão, o Route 53 adiciona os seguintes novos recursos:

- DNS privado para VPCs criadas com o serviço do Amazon Virtual Private Cloud: agora é possível usar o Route 53 para gerenciar seus nomes de domínio internos para VPCs sem

expor os dados de DNS à Internet pública. Para ter mais informações, consulte Trabalhar com zonas hospedadas privadas.

- Motivos de falha na verificação de integridade: agora é possível visualizar o status atual de uma verificação de integridade selecionada, além dos detalhes do que ocasionou a falha na verificação de integridade, conforme relatado em cada verificador de integridade do Route 53. O status inclui o código de status HTTP, e os motivos de falha incluem informações sobre vários tipos de falhas, tais como falhas de correspondência de string e tempos de resposta esgotados. Para ter mais informações, consulte Ver o status e o motivo de falhas da verificação de integridade.
- Conjuntos de delegação reutilizáveis: agora é possível aplicar o mesmo conjunto de quatro servidores de nome autoritativos, conhecidos coletivamente como conjunto de delegação, a várias zonas hospedadas que correspondem a diferentes nomes de domínio. Isso simplifica muito o processo de migração do serviço de DNS para o Route 53 e o gerenciamento de uma grande quantidade de zonas hospedadas. Para utilizar os conjuntos de delegação reutilizáveis, é necessário usar a API do Route 53 ou um SDK da AWS . Para obter mais informações, consulte Referência de API do Amazon Route 53.
- Roteamento de geolocalização aprimorado — Melhoramos ainda mais a precisão do roteamento de geolocalização adicionando suporte para a extensão do edns-client-subnet EDNS0. Para ter mais informações, consulte Roteamento de localização geográfica.
- Suporte ao Signature v4: agora é possível assinar todas as solicitações da API do Route 53 usando o Signature versão 4. Para obter mais informações, consulte Como assinar solicitações de API do Route 53 na Referência da API do Amazon Route 53.

31 de julho de 2014

Com essa versão, você pode fazer o seguinte:

- Registrar novos nomes de domínio com o Amazon Route 53. Para ter mais informações, consulte Registrar e gerenciar novos domínios com o Amazon Route 53.
- Configurar o Route 53 para responder às consultas de DNS com base na geolocalização da qual as consultas são originadas. Para ter mais informações, consulte Roteamento de localização geográfica.

2 de julho de 2014

Com essa versão, você pode fazer o seguinte:

- Editar a maioria dos valores nas verificações de integridade. Para ter mais informações, consulte Criar, atualizar e excluir verificações de integridade.

- Usar a API do Route 53 para obter uma lista dos intervalos IP que os verificadores de integridade do Route 53 usam para verificar a integridade de seus recursos. Você pode usar esses endereços IP para configurar suas regras de roteador e firewall, permitindo que os verificadores de integridade verifiquem seus recursos. Para obter mais informações, consulte GetCheckerIpRangesa Referência de API do Amazon Route 53.
- Atribuir tags de alocação de custos às verificações de integridade, o que também permite a atribuição de nomes a elas. Para ter mais informações, consulte Nomear e adicionar tags às verificações de integridade.
- Use a API do Route 53 para obter o número de verificações de saúde associadas à sua AWS conta. Para obter mais informações, consulte GetHealthCheckCounta Referência de API do Amazon Route 53.

30 de abril de 2014

Com essa versão, agora é possível criar verificações de integridade e usar um nome de domínio em vez de um endereço IP para especificar o endpoint. Isso é útil quando o endereço IP de um endpoint não é fixo ou é atendido por vários IPs, como instâncias do Amazon EC2 ou do Amazon RDS. Para ter mais informações, consulte Criar e atualizar verificações de integridade.

Além disso, algumas informações sobre o uso da API do Route 53; exibidas anteriormente no Guia do desenvolvedor do Amazon Route 53 foram movidas. Agora, toda a documentação da API é mostrada na Referência da API do Amazon Route 53.

18 de abril de 2014

Com esta versão, o Route 53 passará um valor diferente no cabeçalho `Host` quando o valor Port (Porta) da verificação de integridade for 443 e o valor de Procol (Protocolo) for HTTPS. Agora, durante uma verificação de integridade, o Route 53 passa para o endpoint um cabeçalho `Host` que contém o valor do campo Host Name (Nome do host). Se você criou a verificação de integridade usando a ação `CreateHealthCheck` da API, esse será o valor do elemento `FullyQualifiedDomainName`.

Para ter mais informações, consulte Criar, atualizar e excluir verificações de integridade.

9 de abril de 2014

Com essa versão, agora é possível ver a porcentagem de verificadores de integridade do Route 53 identificando a boa integridade de um endpoint.

Além disso, o comportamento da métrica Health Check Status na Amazon CloudWatch agora mostra apenas zero (se seu endpoint não estava íntegro durante um determinado período) ou

um (se o endpoint estava íntegro nesse período). A métrica não mostra mais valores entre 0 e 1 para refletir a porcentagem de verificações de integridade do Route 53 que identificam a boa integridade do endpoint.

Para ter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

18 de fevereiro de 2014

Com esta versão, o Route 53 adiciona os seguintes recursos:

- Limite de failover da verificação de integridade: agora é possível especificar depois de quantas verificações de integridade consecutivas pode haver falha em um endpoint para que o Route 53 considere o endpoint como não íntegro, entre 1 e 10 verificações consecutivas. Um endpoint cuja integridade é inadequada precisa ser aprovado no mesmo número de verificações para que sua integridade passe a ser adequada. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.
- Intervalo de solicitação de verificação de integridade: agora é possível especificar com que frequência o Route 53 envia solicitações a um endpoint para determinar se o endpoint está íntegro. As configurações válidas são 10 segundos e 30 segundos. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

30 de janeiro de 2014

Com esta versão, o Route 53 adiciona os seguintes recursos:

- Verificações de integridade de correspondência de string HTTP e HTTPS: agora, o Route 53 oferece suporte a verificações de integridade que determinam a integridade de um endpoint com base na aparência de uma string especificada no corpo da resposta. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.
- Verificações de integridade de HTTPS: agora, o Route 53 oferece suporte a verificações de integridade para sites somente SSL seguros. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.
- **`UPSERT`** para a ação **`ChangeResourceRecordSets`** da API: ao criar ou alterar registros usando a ação `ChangeResourceRecordSets` da API, é possível usar a ação `UPSERT` para criar um novo registro, se não houver nenhum com determinado nome e tipo, ou atualizar um registro existente. Para obter mais informações, consulte ChangeResourceRecordSetsa Referência de API do Amazon Route 53.

7 de janeiro de 2014

Com essa versão, o Route 53 adiciona suporte para verificações de integridade que determinam a integridade de um endpoint com base na exibição ou não de uma string no corpo da resposta. Para ter mais informações, consulte Como o Amazon Route 53 determina a integridade de uma verificação de integridade.

Versões de 2013

14 de agosto de 2013

Com essa versão, o Route 53 adiciona suporte à criação de registros importando um arquivo de zona com formato BIND. Para ter mais informações, consulte Criar registros importando um arquivo de zona.

Além disso, CloudWatch as métricas das verificações de saúde do Route 53 foram integradas ao console do Route 53 e simplificadas. Para ter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

26 de junho de 2013

Com essa versão, o Route 53 adiciona suporte à integração de verificações de saúde com CloudWatch métricas para que você possa fazer o seguinte:

- Averiguar se uma verificação de integridade foi configurada corretamente.
- Analisar a integridade de um endpoint de verificação de integridade durante um determinado período.
- Configure CloudWatch para enviar um alerta do Amazon Simple Notification Service (Amazon SNS) quando todos os verificadores de saúde do Route 53 considerarem que seu endpoint especificado não está íntegro.

Para ter mais informações, consulte Como monitorar as verificações de integridade usando o CloudWatch.

11 de junho de 2013

Com esta versão, o Route 53 adiciona suporte à criação de registros de alias que encaminham consultas de DNS para nomes de domínio alternativos para distribuições da Amazon. CloudFront Você pode usar esse recurso para nomes de domínio alternativos no apex de zona (example.com) e nomes de domínio alternativos de subdomínios (www.example.com). Para ter

mais informações, consulte Roteamento de tráfego para uma CloudFront distribuição da Amazon usando seu nome de domínio.

30 de maio de 2013

Com esta versão, o Route 53 adiciona suporte à avaliação de integridade dos balanceadores de carga do ELB e das instâncias do Amazon EC2 associadas. Para ter mais informações, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

28 de março de 2013

A documentação sobre as verificações de integridade e o failover foi reescrita para melhorar a usabilidade. Para ter mais informações, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

11 de fevereiro de 2013

Com esta versão, o Route 53 adiciona suporte para failover e verificações de integridade. Para ter mais informações, consulte Criar verificações de integridade do Amazon Route 53 e configurar o failover de DNS.

Versão de 2012

21 de março de 2012

Com esta versão, o Route 53 permite a criação de registros de latência. Para ter mais informações, consulte Roteamento baseado em latência.

Versões de 2011

21 de dezembro de 2011

Com essa versão, o console do Route 53 AWS Management Console permite que você crie um registro de alias escolhendo um Elastic Load Balancer em uma lista em vez de inserir manualmente o ID da zona hospedada e o nome DNS do balanceador de carga. A nova funcionalidade está documentada no Guia do desenvolvedor do Amazon Route 53.

16 de novembro de 2011

Com esta versão, você pode usar o console do Route 53 no AWS Management Console para criar e excluir zonas hospedadas e para criar, alterar e excluir registros. A nova funcionalidade está documentada no Guia do desenvolvedor do Amazon Route 53, conforme aplicável.

18 de outubro de 2011

O Guia de conceitos básicos do Amazon Route 53 foi incorporado no Guia do desenvolvedor do Amazon Route 53, e o Guia do desenvolvedor foi reorganizado para aprimorar a usabilidade.

24 de maio de 2011

Essa versão do Amazon Route 53 apresenta registros de alias (que permitem a criação de alias de apex de zona), registros ponderados, uma nova API (2011-05-05) e um acordo de nível de serviço. Além disso, após seis meses na versão Beta, o Route 53 agora está disponível. Para obter mais informações, consulte a página do produto Amazon Route 53 e Escolher entre registros de alias e não alias no Guia do desenvolvedor do Amazon Route 53.

Versão de 2010

5 de dezembro de 2010

Esta é a primeira versão do Guia do desenvolvedor do Amazon Route 53.

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.